

Adam Hosmer-Henner (NSBN 12779)
 Chelsea Latino (NSBN 14227)
 Jane Susskind (NSBN 15099)
McDONALD CARANO LLP
 100 West Liberty Street, Tenth Floor
 Reno, Nevada 89501
 Telephone: (775) 788-2000
 ahosmerhenner@mcdonaldcarano.com
 clatino@mcdonaldcarano.com
 jsusskind@mcdonaldcarano.com

Serrin Turner (admitted *pro hac vice*)
LATHAM & WATKINS LLP
 1271 Avenue of the Americas
 New York, New York 10022
 Telephone: (212) 906-1200
 serrin.turner@lw.com

*Attorneys for Defendant
 Caesars Entertainment, Inc.*

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

In re: DATA BREACH SECURITY
 LITIGATION AGAINST CAESARS
 ENTERTAINMENT, INC.

Master File No. 2:23-cv-01447-ART-BNW

**DEFENDANT CAESARS
 ENTERTAINMENT, INC.'S MOTION
 TO DISMISS CONSOLIDATED CLASS
 ACTION COMPLAINT**

ORAL ARGUMENT REQUESTED

Defendant Caesars Entertainment, Inc. ("Caesars") hereby moves to dismiss the Consolidated Class Action Complaint ("Complaint" or "CAC") (ECF No. 81) filed by Plaintiffs Dhaman Gill, James Martin, April Elvidge, Monica Blair-Smith, Carey Hylton, Charles Popp, Crystal Brewster, Cynthia Rubner, David Lackey, Isaac Dwek, John Gedwill, Laura McNichols, Thomas McNichols, Mark Huddleston, Miguel Rodriguez, Todd Katz, Virginia Stacy, William Rubner, and Edward Cherveney ("Plaintiffs"). A separate Motion for Leave to Exceed Page Limits with respect to this Motion to Dismiss was filed on September 10, 2024 (ECF No. 89).

The Complaint should be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(1), because Plaintiffs lack Article III standing to pursue their claims; and pursuant to Federal Rules of

1 Civil Procedure 12(b)(6) and 9(b), because the Complaint fails to state a claim. This motion to
2 dismiss is based upon the following memorandum of points and authorities, together with all
3 accompanying documents and exhibits, and such oral argument or other materials as may be
4 presented in connection with the hearing of this matter.

5 Dated: September 12, 2024.

6 McDONALD CARANO LLP

7 /s/ Adam Hosmer-Henner

8 Adam Hosmer-Henner (NSBN 12779)

9 Chelsea Latino (NSBN 14227)

10 Jane Susskind (NSBN 15099)

11 100 West Liberty Street, Tenth Floor

12 Reno, Nevada 89501

13 Telephone: (775) 788-2000

14 ahosmerhenner@mcdonaldcarano.com

15 clatino@mcdonaldcarano.com

16 jsusskind@mcdonaldcarano.com

17 LATHAM & WATKINS LLP

18 Serrin Turner (admitted *pro hac vice*)

19 1271 Avenue of the Americas

20 New York, New York 10022

21 Telephone: (212) 906-1200

22 serrin.turner@lw.com

23 *Attorneys for Defendant*

24 *Caesars Entertainment, Inc.*

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. BACKGROUND	3
A. The Criminal Attack on Caesars	3
B. Caesars' Notification and Remediation Efforts	4
C. Procedural Background.....	5
III. LEGAL STANDARD & CHOICE OF LAW	5
A. Pleading Requirements	5
B. Choice of Law	6
IV. ARGUMENT.....	6
A. Plaintiffs Lack Article III Standing.....	6
B. Plaintiffs Lack Standing For Injunctive Relief	13
C. Plaintiffs Have Failed to Plausibly Allege Damages Cognizable Under Negligence or Contract Law	13
D. Plaintiffs Do Not State a Claim for Negligence.....	14
1. Plaintiffs Fail to Allege Facts Giving Rise to a Duty of Care	14
2. Plaintiffs Do Not Allege a Breach of Duty	17
3. Plaintiffs' Alleged Damages Are Barred by the Economic Loss Doctrine	18
E. Plaintiffs Do Not State an Implied Contract Claim	19
F. Plaintiffs Do Not Plead a Viable Unjust Enrichment Claim.....	21
G. Plaintiffs' Statutory Claims Fail on Numerous Grounds	22
1. Plaintiffs' Misrepresentation-Based Claims Are Uniformly Deficient (Counts IV, V, VI, IX, X, XI, XII, XIII, XV, XVI, XVIII)	22
2. Plaintiffs' Data Breach Notification Statute Claims Fail to Allege Cognizable Harm (Counts VII, VIII, XVII).....	27
H. Plaintiffs' Individual Statutory Claims Fail for Additional Reasons.....	28
1. The Texas Deceptive Practices Act Claim Must Be	

1		Voluntarily Dismissed, or the Entire Case Must Be Abated	28
2	2.	The Nevada Consumer Fraud Act Claim Fails for Additional Reasons	29
3	3.	Plaintiffs’ California Statutory Claims Fail	31
4	a.	Plaintiffs Lack Statutory Standing Under the UCL and CLRA	31
5	b.	Plaintiffs’ UCL Claim Fails on Several Other Grounds.....	33
6	c.	Plaintiffs’ CLRA Claim Fails on Additional Grounds.....	35
7	4.	The Pennsylvania Unfair Trade Practice and Consumer Protection Law Claim Fails	35
8	5.	Virginia Consumer Protection Act.....	36
9	6.	Plaintiffs’ Minnesota Statutory Claims Are Inadequately Pled	37
10	7.	Plaintiffs’ Illinois Statutory Claims Fail	38
11	8.	Plaintiffs’ Claim Under New York General Business Law § 349 Fails.....	39
12			
13			
14			
15	V.	CONCLUSION.....	40
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>Abdale v. N. Shore Long Island Jewish Health Sys., Inc.</i> , 49 Misc. 3d 1027 (Sup. Ct. Queens Cnty. 2015)	39
<i>Ames v. Caesars Entm't Corp.</i> , 2019 WL 1441613 (D. Nev. Apr. 1, 2019)	21
<i>Anderson v. Kimpton Hotel & Rest. Grp., LLC</i> , 2019 WL 3753308 (N.D. Cal. Aug. 8, 2019)	17
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009)	6, 19
<i>Baba v. Hewlett-Packard Co.</i> , 2010 WL2486353 (N.D. Cal. June 16, 2010)	30
<i>Bardin v. DaimlerChrysler Corp.</i> , 136 Cal.App.4th 1255 (2006)	35
<i>Baton v. Ledger SAS</i> , 2024 WL 3447511 (N.D. Cal. July 16, 2024)	16
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	19
<i>Belmont v. MB Inv. Partners, Inc.</i> , 708 F.3d 470 (3d Cir. 2013)	25
<i>Benner v. Bank of America, N.A.</i> , 917 F.Supp.2d 338 (E.D. Pa. 2013)	35
<i>Borenstein v. Animal Found.</i> , 526 F. Supp. 3d 820 (D. Nev. 2021)	16
<i>Brickfire LLC v. Aetna Life Ins. Co.</i> , 2024 WL 1121007 (C.D. Cal. Feb. 16, 2024)	33
<i>Buckland v. Threshold Enters., Ltd.</i> , 155 Cal.App.4th 798 (2007)	35
<i>Casey v. Merck & Co., Inc.</i> , 722 S.E.2d 842 (Va. 2012)	37
<i>Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.</i> , 20 Cal.4th 163 (1999)	35
<i>Clark v. Wells Fargo Home Mortg.</i> , 2014 WL 5297723 (N.D. Tex. Oct. 16, 2014)	29

1	<i>Cruz v. Andrews Restoration, Inc.</i> ,	24
2	364 S.W.3d 817 (Tex. 2012).....	
3	<i>Daniels v. AETC II Privatized Housing LLC</i> ,	29
4	2020 WL 6789336 (W.D. Tex. Jan. 6, 2020)	
5	<i>Daugherty v. Am. Honda Motor Co.</i> ,	25
6	144 Cal. App. 4th 824 (2006)	
7	<i>Davidson v. Apple, Inc.</i> ,	33
8	2017 WL 976048 (N.D. Cal. Mar. 14, 2017).....	
9	<i>Davis v. HSBC Bank Nev., N.A.</i> ,	35
10	691 F.3d 1152 (9th Cir. 2012)	
11	<i>De Bouse v. Bayer</i> ,	39
12	235 Ill. 2d 544 (2009)	
13	<i>Demedice v. CVS Health Corp.</i> ,	38
14	2017 WL 569157 (N.D. Ill. Feb. 13, 2017)	
15	<i>Dugas v. Starwood Hotels & Resorts Worldwide, Inc.</i> ,	27
16	2016 WL 6523428 (S.D. Cal. Nov. 3, 2016)	
17	<i>Ebeid ex rel. U.S. v. Lungwitz</i> ,	6
18	616 F.3d 993 (9th Cir. 2010)	
19	<i>Ebner v. Fresh, Inc.</i> ,	34, 35
20	838 F.3d 958 (9th Cir. 2016)	
21	<i>eFinanzas, S.A.S. v. Roy</i> ,	25
22	2024 WL 1705471 (S.D. Tex. Apr. 4, 2024)	
23	<i>Ehrlich v. BMW of N. Am., LLC</i> ,	24, 35
24	801 F.Supp.2d 908 (C.D. Cal. 2010)	
25	<i>Enslin v. The Coca-Cola Co.</i> ,	16
26	136 F. Supp. 3d 654 (E.D. Pa. 2015), <i>aff'd</i> , 739 F. App'x 91 (3d Cir. 2018)	
27	<i>E-Shops Corp. v. U.S. Bank Nat. Ass'n</i> ,	37
28	678 F.3d 659 (8th Cir. 2012)	
	<i>Falkenberg v. Alere Home Monitoring, Inc.</i> ,	32
	2014 WL 5020431 (N.D. Cal. Oct. 7, 2014).....	
	<i>Flaherty v. Wells Fargo Bank Nat'l Ass'n</i> ,	15
	623 F. Supp. 3d 1124 (D. Nev. 2022).....	
	<i>Flores v. United Parcel Serv., Inc.</i> ,	20
	768 F. App'x 677 (9th Cir. 2019)	
	<i>Flores-Mendez v. Zoosk, Inc.</i> ,	32
	2021 WL 4553772 (N.D. Cal. Oct. 5, 2021).....	

1	<i>Fox v. Iowa Health Sys.,</i>	
2	399 F.Supp.3d 780 (W.D. Wisc. 2019).....	28
3	<i>Gardiner v. Walmart Inc.,</i>	
4	2021 WL 2520103 (N.D. Cal. Mar. 5, 2021).....	20, 32
5	<i>Gonzales v. Uber Techs., Inc.,</i>	
6	305 F.Supp.3d 1078 (N.D. Cal. 2018)	32
7	<i>Gordon v. Finch,</i>	
8	2023 WL 3496427 (N.D. Ind. May 17, 2023)	24
9	<i>Grady v. Progressive Direct Ins. Co.,</i>	
10	643 F. Supp. 3d 929 (D. Minn. 2022).....	23
11	<i>Griffey v. Magellan Health Inc.,</i>	
12	562 F. Supp. 3d 34 (D. Ariz. 2021)	passim
13	<i>Grifo & Co., PLLC v. Cloud X Partners Holdings, LLC,</i>	
14	485 F. Supp. 3d 885 (E.D. Mich. 2020).....	15
15	<i>Grigsby v. Valve Corp.,</i>	
16	2012 WL 5993755 (W.D. Wash. Nov. 14, 2012)	14
17	<i>Guerra v. Dematic Corp.,</i>	
18	2020 WL 5995496 (D. Nev. Oct. 8, 2020)	24
19	<i>Guy v. Tidewater Inv. Props.,</i>	
20	41 Va. Cir. 218 (1996)	25
21	<i>Guzman v. Polaris Indus. Inc.,</i>	
22	49 F.4th 1308 (9th Cir. 2022)	33
23	<i>H&H Pharm., LLC v. Chattem Chemicals, Inc.,</i>	
24	2020 WL 376648 (D. Nev. Jan. 23, 2020).....	21
25	<i>Halcrow, Inc. v. Eighth Jud. Dist. Ct.,</i>	
26	129 Nev. 394 (2013)	18
27	<i>Hamm v. Mercedes-Benz USA, LLC,</i>	
28	2022 WL 913192 (N.D. Cal. Mar. 29, 2022).....	34
	<i>Hammerling v. Google, LLC,</i>	
	615 F.Supp.3d 1069 (N.D. Cal. 2022)	34
	<i>Himan v. Thor Indus., Inc.,</i>	
	2022 WL 683650 (N.D. Ind. Mar. 8, 2022).....	23, 25
	<i>Hines v. Hash,</i>	
	843 S.W.2d 464 (Tex. 1992).....	28
	<i>Hinojos v. Kohl's Corp.,</i>	
	718 F.3d 1098 (9th Cir. 2013)	31

1	<i>Hodsdon v. Mars, Inc.</i> ,	
2	891 F.3d 857 (9th Cir. 2018)	35
3	<i>Horowitz v. Stryker Corp.</i> ,	
4	613 F. Supp. 2d 271 (E.D.N.Y. 2009)	39
5	<i>Houston v. DTN Operating Co., LLC</i> ,	
6	2017 WL 4653246 (E.D. Tex. Oct. 17, 2017)	23
7	<i>In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.</i> ,	
8	2021 WL 5937742 (D.N.J. Dec. 16, 2021)	37
9	<i>In re Anthem, Inc. Data Breach Litig.</i> ,	
10	2016 WL 3029783 (N.D. Cal. May 27, 2016)	24
11	<i>In re Arthur J. Gallagher Data Breach Litig.</i> ,	
12	631 F. Supp. 3d 573 (N.D. Ill. 2022)	22
13	<i>In re Equifax Inc. Sec. Litig.</i> ,	
14	357 F. Supp. 3d 1189 (N.D. Ga. 2019)	17
15	<i>In re Equifax, Inc., Customer Data Sec. Breach Litig.</i> ,	
16	362 F. Supp. 3d 1295 (N.D. Ga. 2019)	26, 30
17	<i>In re Facebook, Inc. Internet Tracking Litig.</i> ,	
18	956 F.3d 589 (9th Cir. 2020)	20
19	<i>In re iPhone App. Litig.</i> ,	
20	6 F.Supp.3d 1004 (N.D. Cal. 2013)	33
21	<i>In re MCG Health Data Sec. Issue Litig.</i> ,	
22	2023 WL 3057428 (W.D. Wash. Mar. 27, 2023)	17
23	<i>In re Mednax Servs., Inc.</i> ,	
24	603 F. Supp. 3d 1183 (S.D. Fla. 2022)	15
25	<i>In re Rutter's Inc. Data Sec. Breach Litig.</i> ,	
26	511 F. Supp. 3d 514 (M.D. Pa. 2021)	24, 25
27	<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> ,	
28	613 F.Supp.3d 1284, 1300 (S.D. Cal. May 7, 2020)	27
	<i>In re Sony Gaming Networks & Customer Data Sec. Breach Litig.</i> ,	
	996 F. Supp. 2d 942 (S.D. Cal. 2014)	24
	<i>In re Sony Gaming Networks and Customer Data Sec. Breach Litig.</i> ,	
	903 F. Supp. 2d 942 (S.D. Cal. 2012)	16, 31
	<i>In re Target Corp. Data Sec. Breach Litig.</i> ,	
	66 F. Supp. 3d 1154 (D. Minn. 2014)	16
	<i>In re Zappos.com, Inc.</i> ,	
	2013 WL 4830497 (D. Nev. Sept. 9, 2013)	19, 22

1	<i>Jackson v. Anheuser-Busch InBev SA/NV, LLC</i> ,	
2	2021 WL 3666312 (S.D. Fla. Aug. 18, 2021).....	23
3	<i>Jarzyna v. Home Props., L.P.</i> ,	
4	185 F. Supp. 3d 612 (E.D. Pa. 2016)	36
5	<i>JL Beverage Co., LLC v. Beam Inc.</i> ,	
6	2017 WL 5158661 (D. Nev. Nov. 7, 2017)	21
7	<i>Johnson v. Bobcat Co.</i> ,	
8	175 F. Supp. 3d 1130 (D. Minn. 2016).....	37
9	<i>Johnson v. Nice Pak Prod., Inc.</i> ,	
10	2024 WL 2845928 (S.D. Ind. June 5, 2024).....	16
11	<i>Kahn v. Walmart Inc.</i> ,	
12	107 F.4th 585 (7th Cir. 2024)	22
13	<i>Kearns v. Ford Motor Co.</i> ,	
14	567 F.3d 1120 (9th Cir. 2009)	22, 33
15	<i>Khoja v. Orexigen Therapeutics, Inc.</i> ,	
16	899 F.3d 988 (9th Cir. 2018)	4
17	<i>Kljajich v. Whirlpool Corp.</i> ,	
18	2015 WL 12838163 (N.D. Ill. Sept. 25, 2015)	38
19	<i>Krottner v. Starbucks Corp.</i> ,	
20	406 F. App'x 129 (9th Cir. 2010)	13
21	<i>Kuhns v. Scottrade, Inc.</i> ,	
22	868 F.3d 711 (8th Cir. 2017)	passim
23	<i>Kwikset Corp. v. Super. Ct.</i> ,	
24	51 Cal.4th 310 (2011)	31, 35
25	<i>Lewert v. P.F. Chang's China Bistro, Inc.</i> ,	
26	819 F.3d 963 (7th Cir. 2016)	38
27	<i>Maag v. U.S. Bank, Nat'l Ass'n</i> ,	
28	2021 WL 5605278 (S.D. Cal. Apr. 8, 2021).....	26
	<i>Mauer v. Am. Home Mortg. Acceptance, Inc.</i> ,	
	2011 WL 6752631 (D. Nev. Dec. 23, 2011).....	24
	<i>Maxwell v. Unilever United States, Inc.</i> ,	
	2014 WL 4275712 (N.D. Cal. Aug. 28, 2014)	33
	<i>McManus v. McManus Fin. Consultants, Inc.</i> ,	
	2012 WL 937812 (D. Nev. Mar. 19, 2012), <i>aff'd</i> , 552 F. App'x 713 (9th Cir.	
	2014)	4
	<i>Mekhail v. N. Mem'l Health Care</i> ,	
	2024 WL 1332260 (D. Minn. Mar. 28, 2024)	23, 37

1	<i>Mizrahi v. Wells Fargo Home Mortg.,</i>	
2	2010 WL 2521742 (D. Nev. June 16, 2010).....	19
3	<i>Moore v. Mars Petcare US, Inc.,</i>	
4	966 F.3d 1007 (9th Cir. 2020) (UCL).....	33
5	<i>Moyer v. Michaels Stores, Inc.,</i>	
6	2014 WL 3511500 (N.D. Ill. July 14, 2014).....	38
7	<i>Nahigian v. Juno Loudoun, LLC,</i>	
8	684 F. Supp. 2d 731 (E.D. Va. 2010)	23
9	<i>O'Shea v. Littleton,</i>	
10	414 U.S. 488 (1974).....	13
11	<i>Orr v. Keystone RV Co.,</i>	
12	2024 WL 2883510 (E.D. Va. June 7, 2024)	24
13	<i>Patel v. Holiday Hosp. Franchising, Inc.,</i>	
14	172 F. Supp. 2d 821 (N.D. Tex. 2001)	29
15	<i>Perdue v. Hy-Vee, Inc.,</i>	
16	455 F. Supp. 3d 749 (C.D. Ill. 2020)	37
17	<i>Peri & Sons Farms, Inc. v. Jain Irr., Inc.,</i>	
18	933 F. Supp. 2d 1279 (D. Nev. 2013).....	18
19	<i>Picus v. Wal-Mart Stores, Inc.,</i>	
20	256 F.R.D. 651 (D. Nev. 2009).....	30
21	<i>Pierce v. N. Dall. Honey Co.,</i>	
22	2020 WL 1047903 (N.D. Tex. Mar. 3, 2020)	29
23	<i>Pirozzi v. Apple, Inc.,</i>	
24	966 F.Supp.2d 909 (N.D. Cal. 2013)	31
25	<i>Polk v. Crown Auto, Inc.,</i>	
26	228 F.3d 541 (4th Cir. 2000)	36
27	<i>Popp v. Cash Station, Inc.,</i>	
28	244 Ill. App. 3d 87 (1st Dist. 1992)	38
	<i>Pruchnicki v. Envision Health Corp.,</i>	
	845 F. App'x. 613 (9th Cir. 2022)	13, 14, 19
	<i>Razuki v. Caliber Home Loans, Inc.,</i>	
	2018 WL 2761818 (S.D. Cal. June 8, 2018).....	20
	<i>Razuki v. Caliber Home Loans, Inc.,</i>	
	2018 WL 6018361 (S.D. Cal. Nov. 15, 2018)	27
	<i>Reid v. Johnson & Johnson,</i>	
	780 F.3d 952 (9th Cir. 2015)	31

1	<i>Rider v. Uphold HQ Inc.</i> ,	
2	657 F.Supp.3d 491 (S.D.N.Y. 2023).....	40
3	<i>Riviello v. Chase Bank USA, N.A.</i> ,	
4	2020 WL 1129956 (M.D. Pa. Mar. 4, 2020).....	36
5	<i>Ruiz v. Gap, Inc.</i> ,	
6	380 F. App'x 689 (9th Cir. 2010)	13
7	<i>Ruiz v. Gap, Inc.</i> ,	
8	540 F. Supp. 2d 1121 (N.D. Cal. 2008)	16
9	<i>Ruiz v. Gap, Inc.</i> ,	
10	622 F. Supp. 2d 908 (N.D. Cal. 2009), <i>aff'd</i> , 380 F. App'x 689 (9th Cir. 2010)	14
11	<i>Sanchez ex rel. Sanchez v. Wal-Mart Stores, Inc.</i> ,	
12	125 Nev. 818 (2009)	14, 16
13	<i>Sharma v. Volkswagen AG</i> ,	
14	524 F. Supp.3d 891 (N.D. Cal. 2021)	21
15	<i>Silver State Broad., LLC v. Crown Castle MU, LLC</i> ,	
16	2018 WL 6606064 (D. Nev. Dec. 17, 2018).....	15
17	<i>Smallman v. MGM Resorts Int'l</i> ,	
18	638 F. Supp. 3d 1175 (D. Nev. 2022).....	15
19	<i>Soffer v. Five Mile Cap. Partners, LLC</i> ,	
20	2013 WL 638832 (D. Nev. Feb. 19, 2013)	30
21	<i>Song v. Champion Petfoods USA, Inc.</i> ,	
22	2020 WL 7624861 (D. Minn. Dec. 22, 2020), <i>aff'd</i> , 27 F.4th 1339 (8th Cir.	
23	2022)	25, 26
24	<i>Sonner v. Premier Nutrition Corporation</i> ,	
25	971 F.3d 834 (9th Cir. 2020)	21, 33
26	<i>Sparks v. Alpha Tau Omega Fraternity, Inc.</i> ,	
27	127 Nev. 287 (2011)	15
28	<i>Spokeo, Inc. v. Robins</i> ,	
	578 U.S. 330 (2016).....	6
	<i>Swarts v. Home Depot, Inc.</i> ,	
	689 F.Supp.3d 732 (N.D. Cal. 2023)	32
	<i>Swartz v. KPMG LLP</i> ,	
	476 F.3d 756 (9th Cir. 2007)	23
	<i>Taddeo v. Taddeo</i> ,	
	2011 WL 4074433 (D. Nev. Sept. 13, 2011)	30
	<i>Tellabs, Inc. v. Makor Issues & Rights, Ltd.</i> ,	
	551 U.S. 308 (2007).....	4

1	<i>Terracon Consultants W., Inc. v. Mandalay Resort Grp.</i> ,	
2	125 Nev. 66 (2009)	18, 19
3	<i>Torres v. Rothstein</i> ,	
4	2020 WL 2559384 (D. Nev. May 20, 2020)	6
5	<i>Troy v. Am. Bar Ass’n</i> ,	
6	2024 WL 1886753 (E.D.N.Y. Apr. 30, 2024)	39
7	<i>Urb. Outfitters, Inc. v. Dermody Operating Co., LLC</i> ,	
8	2022 WL 4134127 (D. Nev. Sept. 12, 2022)	22
9	<i>Vess v. Ciba-Geigy Corp. USA</i> ,	
10	317 F.3d 1097 (9th Cir. 2003)	23
11	<i>Weinberg v. Sun Co., Inc.</i> ,	
12	565 Pa. 612 (2001)	35
13	<i>Williams v. Apple, Inc.</i> ,	
14	449 F.Supp.3d 892 (N.D. Cal. 2020)	33
15	<i>Williams v. Gerber Products, Co.</i> ,	
16	552 F.3d 934 (9th Cir. 2008)	34
17	<i>Winkle Chevy-Olds-Pontiac, Inc. v. Condon</i> ,	
18	830 S.W.2d 740 (Tex. App. 1992)	29
19	<i>Woods v. Maytag Co.</i> ,	
20	2010 WL 4314313 (E.D.N.Y. Nov. 2, 2010)	39
21	<i>Wynn’s Extended Care, Inc. v. Bradley</i> ,	
22	619 F. App’x 216 (4th Cir. 2015)	36
23	<i>Yocca v. Pittsburgh Steelers Sports, Inc.</i> ,	
24	854 A.2d 425 (Pa. 2004)	36
25	<i>Yuille v. Uphold HQ Inc.</i> ,	
26	686 F. Supp. 3d 323 (S.D.N.Y. 2023)	25, 39
27	STATUTES	
28	15 U.S.C. §§ 6501-6505	39
	42 U.S.C. § 1320d	39
	815 Ill. Comp. Stat. § 530/10(a)	27
	Cal. Civ. Code § 1798.82(a)	27
	N.Y. Gen. Bus. Law § 349	39
	Nev. Rev. Stat. § 598.0923(2)	25
	Nev. Rev. Stat. § 603A.210	16

1	Nev. Rev. Stat. § 603A.210(1).....	30
2	Tex. Bus & Com. Code § 17.505.....	28, 29
3	Tex. Bus & Com. Code § 17.505(a)	28
4	Va. Code § 59.1-200	36
5	Va. Code § 59.1-204(A).....	36
6	Va. Code Ann. §§ 18.2-186.6	27

RULES

8	Fed. R. Civ. P. 12(b)(6).....	4, 6
9	Fed. R. Civ. P. 9(b)	6, 22

TREATISES

12	Restatement (Second) of Torts § 314A(1)(a).....	15
----	---	----

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

This case arises from a criminal cyber-extortion attack against Caesars that occurred in August 2023 (the “Attack”). As Plaintiffs’ own allegations make clear, the attackers did not get into Caesars’ network through any vulnerability on Caesars’ own systems; rather, the attackers tricked a third-party IT vendor into providing credentials for certain Caesars’ network accounts, which they then leveraged to steal certain customer information. As Plaintiffs’ allegations further show, the attackers did so in order to extract a ransom from Caesars, not to use the information to commit identity theft against the customers. Indeed, Plaintiffs do not identify any reason to believe that the compromised information has been used to harm customers in any way, or that it is still in the hands of any bad actors. Rather, Plaintiffs acknowledge that Caesars paid a large ransom to the attackers to secure the deletion of the stolen data. They likewise acknowledge that, as an additional precaution, Caesars promptly and proactively offered free, comprehensive identity theft protection and credit monitoring services to all customers potentially impacted by the incident.

While Caesars thus protected its customers from any risk of significant harm from the Attack, Plaintiffs nonetheless saw fit to file this lawsuit. They allege a laundry list of supposed “injuries” they experienced due to the Attack, and have packed the Complaint (ECF No. 81) with 18 causes of action under nine different state laws. However, none of the alleged injuries are sufficient to confer Article III standing or support cognizable injury allegations, and each of their claims is fatally flawed on the merits.

Plaintiffs lack Article III standing. Plaintiffs—who state they are members of Caesars’ Rewards loyalty program who gambled at Caesars properties or online—do not allege any actual injuries to them that can be attributed to the Attack. Instead, their core theory of harm rests on a supposed “*increased risk of fraud, identity theft, and other misuse of their*” personally identifiable information (“PII”). CAC ¶ 10 (emphasis added). But as the Supreme Court’s holding in *TransUnion LLC v. Ramirez* made crystal clear, the “risk of future harm” cannot supply standing for a damages claim. 594 U.S. 413, 415, (2021). Nor can Plaintiffs convert this stated risk of future identity theft into different and independent standing grounds, by conclusorily alleging that they

1 feel “fear” or “anxiety” about that future risk, or by claiming they have taken what amount to
2 unnecessary mitigation measures with respect to that risk, or by vaguely pointing to some sort of
3 financial fraud they have supposedly experienced but cannot plausibly connect to the Attack.
4 Standing requirements would be far too easy to evade if such bootstrapping were sufficient to
5 circumvent them. The Complaint should therefore be dismissed for lack of Article III standing.

6 **Plaintiffs’ claims fail on the merits.** Beyond their lack of standing, each of Plaintiffs’ 18
7 causes of action suffers from fatal defects. As to their common law claims for negligence, breach
8 of implied contract, and unjust enrichment, Plaintiffs do not plausibly plead any wrongdoing by
9 Caesars. Federal courts around the country have repeatedly concluded that simply alleging that a
10 breach occurred does not sufficiently plead that a defendant acted negligently. Further, Plaintiffs
11 fail to allege the existence of any duty Caesars had to prevent third-party criminal conduct like that
12 giving rise to the Attack (negligence), fail to identify a specific contractual term that was breached
13 (implied contract), fail to plead a lack of legal remedies (unjust enrichment), and fail to allege any
14 cognizable damages (or benefit to Caesars, for unjust enrichment) to support these claims.

15 Plaintiffs’ statutory claims fare no better. Nearly every claim is grounded in fraud, but
16 Plaintiffs fail to allege the details of any alleged misrepresentation or omission (much less with
17 the required specificity). Plaintiffs also disregard numerous elements of the statutes they invoke.
18 Many require Plaintiffs to show reliance, but they do not allege they even viewed, let alone relied
19 on, any purported misrepresentations; others require an affirmative duty to disclose, but Plaintiffs
20 do not allege the type of relationship giving rise to such a duty; and still others impose statutory
21 standing requirements that Plaintiffs cannot meet. To top it off, Plaintiffs have attempted to plead
22 a claim under the Texas Deceptive Practices Act without complying with the statute’s pre-suit
23 notice requirement. The remedy for that failure is to abate the *entire lawsuit* until Plaintiffs comply
24 with the statute’s notice provision, or for Plaintiffs to voluntarily dismiss the claim immediately.

25 For these reasons, as detailed below, the case should be dismissed in its entirety.
26
27
28

II. BACKGROUND¹

Caesars is a leading hospitality and gaming company that owns and operates hotel, casino, and resort properties throughout the United States. CAC ¶ 205. Caesars operates a loyalty program, known as Caesars Rewards, that allows members to earn and redeem credits and rewards at more than 50 destinations. *Id.* ¶ 210. Plaintiffs are 19 consumers from nine different states who claim that their PII was compromised when cybercriminals infiltrated Caesars’ computer systems and obtained a copy of Caesars’ Rewards database. *See, e.g., id.* ¶¶ 7, 13-204.

A. The Criminal Attack on Caesars

In August 2023, a criminal hacking group known as Scattered Spider gained access to Caesars’ internal computer network through a “social engineering attack” on a third-party IT support vendor used by Caesars. CAC ¶¶ 2, 224. Specifically, the attackers targeted Caesars’ vendor through the use of “convincing phone calls” impersonating legitimate Caesars employees, convincing third-party helpdesk employees to reset account credentials and turn over control of them to the attackers. *Id.* The attackers leveraged these credentials to gain access to Caesars’ systems and illegally obtain a copy of the Rewards database that contained certain personal information of Rewards members. *Id.* ¶ 225.

Plaintiffs acknowledge that the Attack was a cyber-extortion attack, meaning that the data was exfiltrated for purposes of collecting a ransom payment in return for its deletion. *Id.* ¶¶ 226, 269. After verifying that the threat actor had exfiltrated data from Caesars’ loyalty program database, Caesars agreed to pay the attackers in exchange for the attackers refraining from publishing or further disseminating the exfiltrated data. *Id.* ¶ 6. Plaintiffs do not allege or provide any evidence that the exfiltrated data has been published, sold, marketed, or otherwise distributed to third parties following the attack—and Caesars is similarly unaware of any actual or attempted misuse of personal information arising from the attack.

Plaintiffs make conclusory allegations throughout the Complaint that the occurrence of the breach indicates that Caesars failed to comply with industry security standards. *See, e.g., id.* ¶¶

¹ For purposes of this Motion to Dismiss, Caesars accepts, as it must, the factual allegations in the CAC as true.

252-268. However, Plaintiffs make no allegation about the cause of the attack other than that it resulted from a social engineering attack on Caesars' third-party IT vendor. In particular, they do not identify any specific, allegedly deficient security practices by Caesars that supposedly allowed the attackers to infiltrate Caesars' systems.

B. Caesars' Notification and Remediation Efforts

When Caesars discovered the Attack on August 18, 2023, Caesars quickly "activated [its] incident response protocols," "implemented a series of containment and remediation measures," "notified law enforcement," and "engaged leading cybersecurity firms" to assist in its investigation. *See* Caesars Entertainment, Inc. Form 8-K, Report of Unscheduled Material Events or Corporate Event (Sept. 14, 2023) at 2 ("Form 8-K")² (cited in CAC ¶ 228 n. 21)³; *see also id.* ¶¶ 224-225. Plaintiffs do not allege that the Attack compromised Caesars' customer-facing operations, or that Caesars lost control of or access to its internal IT systems. *Id.*

After a preliminary investigation, Caesars publicly reported the attack on September 14, 2023 through a form 8-K filing with the SEC and on a public informational website. CAC ¶¶ 228-229; *see also* Form 8-K. Caesars informed customers the attackers had obtained a copy of Caesars' "loyalty program database," and that the stolen information included "driver's license numbers and/or social security numbers" for some Rewards members in the database, but did not include any member passwords/PINs, bank account information, or payment card information. Form 8-K at 2; *id.* ¶ 229.. Caesars confirmed that it had taken proactive "steps to ensure that the stolen data [was] deleted by the unauthorized actor," which Plaintiffs allege included a \$15 million ransom

² <https://investor.caesars.com/static-files/0bc13ee5-34a9-402e-8e7a-824b9dba4e57>.

³ The Court may consider Caesars' Form 8-K in resolving this motion. As the Supreme Court has held, "courts must consider the complaint in its entirety, as well as other sources courts ordinarily examine when ruling on Rule 12(b)(6) motions to dismiss, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007). A document is incorporated by reference into a complaint "if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claims." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1002 (9th Cir. 2018) (citations omitted). Here, the Complaint cites extensively to the Form 8-K as the basis for many of its allegations concerning the Attack, the nature of the putative class, and Caesars' notifications concerning the Attack (*see, e.g.*, CAC ¶¶ 1, 228, 232), and thereby incorporates the Form 8-K by reference. *See, e.g., McManus v. McManus Fin. Consultants, Inc.*, 2012 WL 937812, at *4 (D. Nev. Mar. 19, 2012) (considering Form 8-K relied upon by complaint and submitted by defendants), *aff'd*, 552 F. App'x 713 (9th Cir. 2014).

1 payment to secure the deletion of the stolen data. Form 8-K at 2; CAC ¶ 226. Caesars also
 2 confirmed that, notwithstanding those efforts, it would be offering “free credit monitoring and
 3 identity theft protection services” to all Rewards members, and provided instructions for members
 4 to register for those services. CAC ¶ 229; Form 8-K at 2.

5 Beginning on October 6, 2024, once it had determined the identities of individuals whose
 6 PII was potentially impacted, Caesars followed up with individual notifications to potentially
 7 affected customers. CAC ¶ 230. Those notices reiterated that Caesars was offering “complimentary
 8 identity theft protection services for two years,” including “credit and dark web monitoring to help
 9 detect misuse of your information, as well as a \$1,000,000 insurance reimbursement policy and
 10 fully managed identity restoration in the event that you fall victim to identity theft.” CAC ¶ 6 n.
 11 12; ¶ 230 n. 24) (citing Caesars’ “Sample Data breach Notice”). Customers were given
 12 “instructions” for “activat[ing] these services,” and reminded of other ways to remain “vigilant
 13 against identity theft and fraud” that are “always good practice” for anyone. *Id.*; *see also id.* ¶ 231.

14 **C. Procedural Background**

15 On September 15, 2023—the day after Caesars filed its 8-K announcing the data breach—
 16 plaintiffs began filing lawsuits relating to the incident, which reflected little detail or investigation
 17 beyond what appeared in the Form 8-K. *See* ECF No. 1 (*Rodriguez* complaint). After consolidation
 18 of nearly two dozen cases in this Court and appointment of lead counsel, Plaintiffs filed their
 19 Consolidated Complaint. The Consolidated Complaint asserts 18 claims on behalf of a putative
 20 nationwide class and numerous state subclasses, consisting of U.S. consumers whose PII was
 21 allegedly compromised in the breach. CAC ¶¶ 307-323. Plaintiffs assert common law claims for
 22 negligence, breach of implied contract, and unjust enrichment, and assert statutory fraud and
 23 consumer protection act claims under nine different state’s laws.

24 **III. LEGAL STANDARD & CHOICE OF LAW**

25 **A. Pleading Requirements**

26 **Rule 12(b)(1).** To establish Article III standing, a plaintiff must “have (1) suffered an
 27 injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is
 28 likely to be redressed by a favorable judicial decision.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338

(2016). An injury in fact must be both “concrete and particularized.” *Id.* at 339. “For an injury to be ‘particularized,’ it ‘must affect the plaintiff in a personal and individual way.’” *Id.* (citation omitted). To be “concrete,” the injury “must actually exist” and be “‘real,’ and not ‘abstract.’” *Id.* at 340 (citation omitted).

Rule 12(b)(6). To survive a motion to dismiss under Rule 12(b)(6), a complaint must contain “sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). The standard “demands more than an unadorned, the defendant-unlawfully-harmed-me accusation”; mere “labels and conclusions” or a “formulaic recitation of the elements of a cause of action will not do.” *Id.* The standard is higher for claims sounding in fraud. Those claims require the plaintiff to plead “with particularity,” Fed. R. Civ. P. 9(b), which requires Plaintiffs to “state with particularity the circumstances constituting fraud or mistake, including the who, what, when, where, and how of the misconduct charged.” *Torres v. Rothstein*, 2020 WL 2559384, at *3 (D. Nev. May 20, 2020) (quoting *Ebeid ex rel. U.S. v. Lungwitz*, 616 F.3d 993, 998 (9th Cir. 2010)).

B. Choice of Law

None of the Plaintiffs are from Nevada, and all of them claim injuries that, although non-cognizable for the reasons explained below, allegedly occurred in their home states. Despite that, each of the Plaintiffs alleges common law claims—negligence, breach of implied contract, and unjust enrichment—only under Nevada law. CAC ¶ 310. For purposes of this Motion to Dismiss, therefore, Caesars addresses these claims as pled, and demonstrates that Nevada law provides Plaintiffs with no avenue for relief.

IV. ARGUMENT

A. Plaintiffs Lack Article III Standing

In *TransUnion*, the Supreme Court unequivocally held that “in a suit for damages, the mere risk of future harm, standing alone, cannot qualify as concrete harm.” 594 U.S. at 436. Rather, plaintiffs may sue only if a “risk of future harm *materializes* and the individual suffers a concrete harm,” in which case “the harm itself, and not the pre-existing risk, will constitute a basis for the person’s injury and for damages.” *Id.* (emphasis added).

1 The CAC repeats, nearly verbatim, a laundry list of purported “injuries” for each named
 2 Plaintiff. CAC ¶¶ 18, 29, 39, 50, 60, 70, 81, 91, 101, 110, 120, 129, 139, 150, 161, 170, 179, 189,
 3 200. But the primary injury alleged is an “increased risk of fraud, identity theft, and other misuse
 4 of [Plaintiffs’] PII”. *See, e.g.*, CAC ¶¶ 10, 18. To the extent the CAC states that Plaintiffs have
 5 actually experienced identity theft, their own allegations belie their conclusory assertions. None of
 6 the facts they allege support any inference that any Plaintiff has actually had their identity stolen,
 7 through online account compromise, phishing emails, or otherwise—much less due to the Attack.
 8 And Plaintiffs cannot bootstrap their way into Article III standing by claiming “anxiety” based on
 9 the hypothetical risk of future identity theft, alleging “mitigation” costs or efforts they undertook
 10 that were unnecessary given the free forms of protection offered to them by Caesars, or pointing
 11 to unauthorized charges that have no apparent or plausible connection to the Attack.

12 **Risk of identity theft and fraud.** Plaintiffs repeatedly allege that they have been exposed
 13 to an “increased risk of fraud, identity theft, and other misuse of their PII.” *See, e.g.*, CAC ¶ 10.
 14 These allegations cannot establish standing in light of *TransUnion*, which made clear that, to
 15 support standing, the risk needs to actually “materialize.” *TransUnion*, 594 U.S. at 436. Plaintiffs
 16 here lack standing because the risk of fraud has not materialized into any actual, concrete harm.
 17 Indeed, ten out of nineteen named Plaintiffs have not even alleged *attempted* fraud.⁴ The other nine
 18 Plaintiffs reference purported “attempts” at fraud they experienced at some point, but none of those
 19 “attempts” resulted in Plaintiffs actually having their identities stolen, or suffering any actual,
 20 unreimbursed monetary injury—let alone one traceable to the Attack.⁵

21 The “attempts” never became anything more than “attempts” because—apparently due to
 22 effective monitoring and protection offered by Plaintiffs’ credit card providers—Plaintiffs are
 23 never alleged to have paid for any fraudulent transactions. Nor could Plaintiffs claim any injury
 24 even absent such third-party protection, because *Caesars* also offered Plaintiffs two years of
 25 complimentary credit and dark web monitoring—which is still active today for anyone who signed

26 ⁴ These are Plaintiffs Elvridge, Popp, Laura McNichols, Thomas McNichols, Cherveney, C.
 27 Rubner, W. Rubner, Dwek, Blair-Smith, and Lackey.

28 ⁵ These are Plaintiffs Gill ¶ 19, Hylton, ¶ 30, Rodriguez, ¶ 40, Gedwill, ¶ 71, Stacy, ¶ 102, Martin,
 ¶ 121, Brewster, ¶ 151, Katz, ¶ 180, and Huddleston, ¶ 190.

up—along with a \$1 million insurance reimbursement policy and fully managed identity restoration. At least one Plaintiff accepted Caesars’ offer, and it was open to all others. CAC ¶ 187. Accordingly, Plaintiffs cannot show any risk of fraud has “materialize[d]” into a “concrete harm.” *TransUnion*, 594 U.S. at 436; *Ruiz v. Gap, Inc.*, 2009 WL 250481, at *3 (N.D. Cal. Feb. 3, 2009) (no standing where plaintiffs “could contact [defendant] to get reimbursed for” cost of credit monitoring), *aff’d*, 380 F. App’x 689 (9th Cir. 2010); *Whalen v. Michael Stores Inc.*, 153 F. Supp. 3d 577, 580 (E.D.N.Y. 2015) (no standing where plaintiff had “not alleged that she suffered any unreimbursed charges”), *aff’d*, 689 F. App’x 89 (2d Cir. 2017).

These facts also preclude Plaintiffs from establishing any injury based on out-of-pocket costs or time spent on mitigation, *e.g.*, CAC ¶ 28. Plaintiffs “cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 416 (2013). Many of the purported mitigation measures are unreasonable in their own right, such as threadbare allegations that Plaintiff Rodriguez had to close his own bank account just because someone tried to open an account in his name at a *different* bank, CAC ¶ 40, or that Plaintiff Brewster “sign[ed] up for credit monitoring,” CAC ¶ 149, despite already having credit monitoring “at the time of the Data Breach,” CAC ¶ 147. In any event, Plaintiffs cannot allege *any* out-of-pocket costs or mitigation measures that were reasonably necessary in light of Caesars’ offer of comprehensive mitigation services, which Plaintiffs do not allege were inadequate.⁶ *Ruiz v. Gap, Inc.*, 2009 WL 250481, at *3 (N.D. Cal. Feb. 3, 2009) (no standing where defendant had offered to pay or reimburse charges for credit reporting and fraud assistance), *aff’d*, 380 F. App’x 689 (9th Cir. 2010).

In addition, the supposed fraud attempts have no plausible nexus to the Attack. Plaintiffs offer no allegations to support traceability, apart from conclusory assertions that the attempts occurred “as a result of the Data Breach,” *e.g.*, CAC ¶¶ 19, 30, 40, 71, 102, 121, 151, 180, 190. Most of these nine named Plaintiffs do not even specify when the supposed fraud attempts occurred

⁶ The CAC inexplicably asserts that Plaintiff Hylton “attempt[ed] to purchase the credit monitoring service offered by Caesars (but was denied enrollment in such service).” CAC ¶ 27. That allegation makes no sense, because the service was “free”—no purchase necessary—and Plaintiff Huddleston was able to sign up despite unspecified “difficulties registering.” CAC ¶ 187.

or if they postdated the Attack, CAC ¶¶ 30, 71, 102, 121, and out of the others, only Plaintiff Brewster actually alleges the supposed attempts “did not occur before the Data Breach,” CAC ¶ 151. Many of the supposed fraud attempts, moreover, have nothing to do with the PII at issue. In particular, Plaintiffs offer no explanation for how unauthorized charges are supposed to be traceable to the Attack, which is not alleged to have included any payment card or banking information. *See* CAC ¶¶ 30, 121, 151, 180. As another example, while Plaintiff Gedwill’s putative injury consists of “a phishing attempt in which a stranger sent him money and requested that he return it,” CAC ¶ 71; the CAC provides no detail on how that incident plausibly resulted from the Data Breach (or how *being sent* money supposedly harmed him). A stranger would not need Plaintiff Gedwill’s social security number, for instance, in order to send him money; perhaps they might need his banking information—but the data compromised in the Attack did not include such information. *See In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 31 (D.D.C. 2014) (rejecting allegations of fraudulent charges where “[n]o one allege[d] that credit-card, debit-card, or bank-account information was on the stolen tapes”); *Antman v. Uber Techs., Inc.*, 2018 WL 2151231, at *9 (N.D. Cal. May 10, 2018) (no standing where exposed information was not the type needed to commit the fraudulent acts alleged).

Plaintiffs cannot plausibly allege traceability because they have no indication the loyalty program database was ever disclosed or misused. The CAC alleges that, “[u]pon information and belief, the hackers stole PII from Caesars with the specific intent to use it for illicit purposes and/or sell it to others to be misused.” CAC ¶ 269. But the CAC also recognizes that hackers have *already* “carried out this intent” by demanding a ransom to delete the data, which Caesars paid. CAC ¶ 269. The CAC speculates that deletion was not “guarantee[d],” ¶ 6, and that the attackers “may double-dip,” CAC ¶ 224. But Plaintiffs do not allege or cite to any evidence that the data was actually sold, marketed, or distributed further after the Attack. Absent such facts, Plaintiffs have no basis to trace any thinly pled allegations of financial fraud to an attack that was instead aimed at extracting a ransom. *See In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *5 (W.D.N.Y. Feb. 2, 2022) (rejecting standing in case where “a massive amount of data was copied by a hacker and held hostage for payment of a fee,” finding that “plaintiffs do not plausibly allege

that this data breach was the type of cyber-attack targeted to obtain confidential information for purposes of identity theft, as opposed to garden-variety ransomware attack”); *see also, e.g., Patterson v. Med. Rev. Inst. of Am., LLC*, 2022 WL 2267673, at *3 (N.D. Cal. June 23, 2022) (no standing without allegations that hackers “actually viewed” or misused information, where facts instead indicated they “demanded a ransom” and returned data after receiving payment); *Quintero v. Metro Santurce, Inc.*, 2021 WL 5855752, at *7 (D.P.R. Dec. 9, 2021) (hackers encrypting data to demand ransom did not constitute “acquisition and misuse” necessary to support standing); *Travis v. Assured Imaging LLC*, 2021 WL 1862446, at *9 (D. Ariz. May 10, 2021) (ransomware attack did not give rise to injury supporting standing).

Damage and loss of value of PII. Plaintiffs cannot allege a concrete and particularized injury based on the supposed “value” of their PII. In order to survive a motion to dismiss on this theory of harm, a plaintiff “must establish both the existence of a market for her personal information *and an impairment of her ability to participate in that market.*” *Pruchnicki v. Envision Healthcare Corp.*, 439 F. Supp. 3d 1226, 1234 (D. Nev. 2020), *aff’d*, 845 F. App’x 613 (9th Cir. 2021) (quoting *Svenson v. Google Inc.*, 2016 WL 8943301, at *9 (N.D. Cal. Dec. 21, 2016)) (emphasis added). Plaintiffs allege a “market exists for stolen PII ... on the dark web and through illicit criminal networks.” CAC ¶ 277. But Plaintiffs do not suggest they ever would participate themselves in this illicit market, by hawking their own “stolen PII” to criminal networks on the dark web—and any such suggestion would be patently absurd. For similar reasons, the unparticularized and speculative assertion that Plaintiffs might “lose the ability to negotiate sharing their PII for services,” CAC ¶ 285, makes no sense: Consumers do not “negotiate” for “services” based on the “value” of things like their Social Security number, nor do Plaintiffs claim they ever have done or will do so. Plaintiffs also allege the value of PII can be measured by “the economic benefit consumers derive from being able to use it,” and that their PII is now “encumbered” by fraud. ¶ 284. This allegation does not meet the requirements explained in *Pruchnicki*, 439 F. Supp. 3d at 1234, and in any event the CAC fails to allege any instance where a Plaintiff has actually been “denied credit” or “unable to open an electronic account.” CAC ¶ 284. This instead is another theory based on a supposed risk of future harm rather than a harm that has actually materialized.

Benefit of bargain damages. Plaintiffs fail to allege any cognizable “benefit of the bargain” injury stemming from Caesars’ alleged failure to provide adequate security for their data. As an initial matter, the CAC does not plausibly allege that Caesars’s data security was actually inadequate in the first place. *See infra* § IV.D.2. But regardless, Plaintiffs’ theory—that “they would not have stayed at Caesars properties or would have paid less than they did for their rooms” had they known Caesars’ data was insufficient CAC ¶ 290—fails for multiple reasons. Out of nineteen named Plaintiffs, only *six* are ever alleged to have actually stayed at a Caesars property.⁷ The other thirteen have not alleged to have “stayed at Caesars properties” at all, and thus could not possibly have “paid less than they did for their rooms,” since they never purchased any rooms. CAC ¶ 290. Even those six named Plaintiffs who did purchase hotel rooms received exactly what they paid for, a hotel room. And any stolen PII was allegedly bargained not for a hotel room or other goods, but for participation (at no cost) in the Caesars Rewards Program—which, again, is exactly what Plaintiffs received. Plaintiffs therefore fail to show the price “incorporated some particular sum that was understood by both parties to be allocated towards the protection of customer data.” *In re Zappos.com, Inc.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015); *see also Carlsen v. GameStop, Inc.*, 112 F. Supp. 3d 855, 862 (D. Minn. 2015) (no standing for unjust enrichment claim where plaintiff did not show he “bargain[ed] for data privacy/security”); *In re Sci. Applications Int’l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 30 (D.D.C. 2014) (allegations “that some indeterminate part of [the price] went toward paying for security measures” were “too flimsy to support standing”).

Remaining purported injuries. Plaintiffs cannot establish standing based on nuisance, emotional or privacy injuries either. Each of these theories is foreclosed by law. Allegations that Plaintiffs “experienc[ed] an increase in spam calls, texts, and/or emails,” *e.g.*, CAC ¶ 20, do not help their cause, “because receiving spam or mass mail does not constitute an injury,” *Jackson v. Loews Hotels, Inc.*, 2019 WL 6721637, at *4 (C.D. Cal. July 24, 2019) (citing *Peters v. St. Joseph Servs. Corp.*, 74 F. Supp. 3d 847, 857 (S.D. Tex. 2015) (no injury despite plaintiff receiving

⁷ These are Plaintiffs Gill, ¶ 13, Hylton, ¶ 24, Martin, ¶ 115, Cynthia Rubner, ¶ 125, William Rubner, ¶ 134, and Blair-Smith, ¶ 166.

“target[ed]” physical, electronic, and telephonic “solicitations”); *Cherny v. Emigrant Bank*, 604 F. Supp. 2d 605, 609 (S.D.N.Y. 2009) (“The receipt of spam by itself, however, does not constitute a sufficient injury entitling [plaintiff] to compensable relief.”).

Plaintiffs do not have standing based on vague allegations of emotional injury either. *See, e.g.*, CAC ¶ 18 (Plaintiff Gill alleging “daily fear and anxiety about what he may face next”). “[C]ourts have deemed emotional distress too speculative to constitute a measure of damages in data breach cases.” *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2020 WL 4212811, at *16 (N.D. Cal. July 22, 2020) (citing *Pruchnicki*, 439 F. Supp. 3d at 1234); *see also Holly v. Alta Newport Hosp., Inc.*, 2020 WL 6161457, at *3-4 (C.D. Cal. Oct. 21, 2020) (dismissing negligence claim based on “conclusory and vague” claims of “emotional harm and distress”). Finally, “invasion of privacy” or “theft of [Plaintiffs’] PII,” *e.g.*, CAC ¶ 50, cannot confer standing because “[l]oss of privacy and confidentiality are present in every data breach case, and standing alone, they don’t demonstrate a concrete injury,” *F.S. v. Captify Health, Inc.*, 2024 WL 1282437, at *4 (D. Kan. Mar. 26, 2024).

Plaintiffs also cannot establish standing based on invasion of privacy (also called intrusion upon seclusion). While that can be a “traditionally recognized harm,” there is no “close historical or common law analogue” as required to support standing where (as here) “it is not defendants who improperly accessed plaintiffs’ data, but instead other, unauthorized third parties.” *Aponte v. Ne. Radiology, P.C.*, 2022 WL 1556043, at *5 (S.D.N.Y. May 16, 2022). Plaintiffs’ alleged privacy injury also fails because Plaintiffs cannot allege disclosure of PII “to more than individuals or small groups.” *Demarco v. BAC Home Loans Servicing, LP*, 2011 WL 2462209, at *3 (D. Nev. June 17, 2011). Plaintiffs have not alleged, for example, that the PII was posted and viewable publicly. Even if it were “disclosed” to Scattered Spider, Plaintiffs cannot claim privacy-based injuries “simply because there was a data breach.” *Masterson v. IMA Fin. Grp., Inc.*, 2023 WL 8647157, at *5 (D. Kan. Dec. 14, 2023); *see also In re Practicefirst Data Breach Litig.*, 2022 WL 354544, at *7-8 (W.D.N.Y. Feb. 2, 2022) (“[T]his theory of standing has been rejected in the data breach context where, like in this case, plaintiffs have failed to demonstrate any concrete or particularized injury associated with the disclosure.”). That is all Plaintiffs ultimately allege.

1 Plaintiffs are therefore unable to establish standing for all of their claims, and the whole
2 CAC should be dismissed.

3 **B. Plaintiffs Lack Standing For Injunctive Relief**

4 In addition, Plaintiffs lack standing to seek injunctive relief because they cannot show a
5 “real and immediate threat of repeated injury.” *O’Shea v. Littleton*, 414 U.S. 488, 496 (1974).
6 Indeed, given the nature of the Attack, Caesars’ efforts to secure the data and prevent further
7 dissemination, and the passage of over a year with no concrete, adverse effects, Plaintiffs cannot
8 show an imminent risk of future harm from *this* data breach. *See supra* at §IV.A. That failure
9 forecloses any possibility that they could show a “sufficiently imminent and substantial” risk of
10 harm from a *future* act of identity theft or fraud. *TransUnion*, 594 U.S. at 435. And any possible
11 risk from a future data breach is especially speculative given the unique nature of the Attack and
12 fact that Caesars immediately implemented corrective measures. Accordingly, Plaintiffs cannot
13 show the immediate threat of repeated injury necessary to obtain prospective relief.

14 **C. Plaintiffs Have Failed to Plausibly Allege Damages Cognizable Under**
15 **Negligence or Contract Law**

16 A common deficiency that cuts across Plaintiffs’ common law claims (Counts I-III) is that
17 they fail to allege any type of injury cognizable under state negligence and contract law. These
18 claims require as an element “cognizable damages” as a result of Caesars’ conduct. *Pruchnicki*,
19 439 F. Supp. 3d at 1231. Even where a plaintiff alleges an injury-in-fact for purposes of Article III
20 standing, the plaintiff still fails to state a state-law claim where the alleged injuries “stem from the
21 danger of future harm.” *Krottner v. Starbucks Corp.*, 406 F. App’x 129, 131 (9th Cir. 2010)
22 (dismissing negligence claim under Washington law); *see also Pruchnicki v. Envision Health*
23 *Corp.*, 845 F. App’x. 613, 614 (9th Cir. 2022) (“Although [plaintiff] alleged sufficient injury-in-
24 fact to support standing, whether the allegations adequately alleged compensable damages is a
25 different question.”). Nominal damages, speculative harm, or the threat of harm do not suffice to
26 plead a cognizable injury under negligence or contract law; rather, Plaintiffs must plead
27 “nonspeculative,” “appreciable and actual damage.” *Ruiz v. Gap, Inc.*, 380 F. App’x 689, 691-2
28 (9th Cir. 2010); *see also Pruchnicki*, 845 F. App’x. at 615 (dismissing negligence-based, contract-

1 based, and deceptive practices claims under Nevada law for failure to allege cognizable damages).

2 As discussed *supra*, Section IV.A, Plaintiffs do not allege that they personally incurred any
 3 actual damage at all. For example, they do not allege that they have suffered unreimbursed fraud
 4 or identity theft, nor do they allege that they that they incurred any necessary, out-of-pocket losses
 5 aside from voluntarily imposed “mitigation” expenses. That is insufficient. Where “personal
 6 information is compromised due to a security breach, there is no cognizable harm absent actual
 7 fraud or identity theft.” *Grigsby v. Valve Corp.*, 2012 WL 5993755, at *2 (W.D. Wash. Nov. 14,
 8 2012) (dismissing negligence claim); *see also Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917-18 (N.D.
 9 Cal. 2009), *aff’d*, 380 F. App’x 689, 692-93 (9th Cir. 2010) (no actionable contract or negligence
 10 injury when plaintiff “has no actual damages to mitigate since he has never been a victim of
 11 identity theft”); *Pruchnicki*, 845 F. App’x. at 615 (dismissing claims for negligence, implied
 12 contract, and deceptive practices where the plaintiff had not alleged that she suffered identity theft
 13 or fraud or any out-of-pocket losses supported by non-conclusory allegations).

14 So too here. Plaintiffs’ conclusory allegations—of “attempted” fraud and an “increased
 15 risk” of identity theft, CAC ¶ 10—do not plead the requisite nonspeculative, appreciate and actual
 16 injury. The absence of any allegations that Plaintiffs themselves suffered actual, appreciable
 17 damages alone defeats their negligence and contract-based claims.

18 **D. Plaintiffs Do Not State a Claim for Negligence**

19 Plaintiffs’ negligence claim fails because they do not allege facts giving rise to a legal duty
 20 of care, specify any breach of such a duty by Caesars, or plead any cognizable damages.⁸

21 **1. Plaintiffs Fail to Allege Facts Giving Rise to a Duty of Care**

22 Plaintiffs claim that Caesars had a duty “to safeguard[], secur[e], and protect[]” Plaintiffs’
 23 PII from being exposed to cybercriminals. CAC ¶ 328. Nevada law, however, imposes no general
 24 duty “to control the dangerous conduct of another or to warn others of the dangerous conduct.”
 25 *Sanchez*, 125 Nev. at 824. In these circumstances, courts will recognize a duty of care only where

27 ⁸ Under Nevada law, a negligence claim requires “four elements: (1) the existence of a duty of
 28 care, (2) breach of that duty, (3) legal causation, and (4) damages.” *Sanchez ex rel. Sanchez v. Wal-*
Mart Stores, Inc., 125 Nev. 818, 824 (2009).

“(1) a special relationship exists between the parties or between the defendant and the identifiable victim, and (2) the harm created by the defendant’s conduct is foreseeable.” *Id.* Yet neither of the two narrow kinds of special relationships that Courts have traditionally found applies here. *First*, a duty might exist if the defendant had the right or ability to “control” the plaintiff’s or the criminal’s conduct. *See Sparks v. Alpha Tau Omega Fraternity, Inc.*, 127 Nev. 287, 299 (2011) (no duty where plaintiffs or third party were not under defendant’s control). But Caesars obviously had no power to control a third-party criminal hacker. *See Flaherty v. Wells Fargo Bank Nat’l Ass’n*, 623 F. Supp. 3d 1124, 1129 (D. Nev. 2022) (no special relationship where “[plaintiff] was induced by the scammers, not Wells Fargo, to wire the \$30,000 into [an] account” controlled by criminals). *Second*, a duty can arise where the plaintiff is dependent on the defendant, like passengers are dependent on common carriers, or a “guest” can be dependent on an “innkeeper.” Restatement (Second) of Torts § 314A(1)(a). But Nevada courts have never extended any such special relationship to cover the type of conduct at issue here, where online criminal activity allegedly leads to nonphysical harms. *See Grifo & Co., PLLC v. Cloud X Partners Holdings, LLC*, 485 F. Supp. 3d 885, 898 (E.D. Mich. 2020) (declining to extend “special relationship” doctrine to cover ransomware attack “without the benefit of any Michigan precedent on point”).

Far from a special relationship, Plaintiffs’ relationship with Caesars is quintessentially economic—each Plaintiff alleges that they “regularly gambled” with Caesars, both in person and online, and joined Caesars’ Rewards program to earn perks from that activity. *See, e.g.*, CAC ¶¶ 13, 24, 35, 45, 55, 65, 76, 86, 96, 106, 115, 144, 156, 166, 175, 185, 196. But a “‘straightforward vendor-vendee relationship,’ or an association characterized by ‘routine, arms-length dealings’ will not suffice to establish a special relationship.” *Silver State Broad., LLC v. Crown Castle MU, LLC*, 2018 WL 6606064, at *3 (D. Nev. Dec. 17, 2018). Trying to avoid this rule, Plaintiffs claim that a special relationship arose simply because they provided their PII to Caesars, and that Caesars was in an “exclusive position” to protect it. CAC ¶ 329. But the mere “transmittal of PII alone” does not “transform[]” a business relationship into a special one. *Smallman v. MGM Resorts Int’l*, 638 F. Supp. 3d 1175, 1194 (D. Nev. 2022); *see also In re Mednax Servs., Inc.*, 603 F. Supp. 3d 1183, 1226 (S.D. Fla. 2022) (the “mere receipt of confidential information is insufficient by itself

1 to transform an arm’s-length transaction into a fiduciary relationship”).

2 Instead, whether a special relationship can be based on control over *property* (as Plaintiffs
3 seem to treat PII)—as opposed to control over persons and locations—depends on “the creation of
4 a bailment.” *Borenstein v. Animal Found.*, 526 F. Supp. 3d 820, 838 (D. Nev. 2021). But PII is not
5 a type of “property”—it is certainly not recognized as such for bailment purposes—nor do Plaintiffs
6 allege that Caesars exercised the requisite *exclusive* possession of their PII, or agreed but failed to
7 return it. *See Enslin v. The Coca-Cola Co.*, 136 F. Supp. 3d 654, 679 (E.D. Pa. 2015) (“PII lost by
8 a party holding that information was not ‘property’ or ‘personalty’ for the purposes of the law of
9 bailment”), *aff’d*, 739 F. App’x 91 (3d Cir. 2018); *In re Sony Gaming Networks and Customer*
10 *Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 974-75 (S.D. Cal. 2012) (similar); *Ruiz v. Gap, Inc.*,
11 540 F. Supp. 2d 1121, 1126-27 (N.D. Cal. 2008) (similar); *Johnson v. Nice Pak Prod., Inc.*, 2024
12 WL 2845928, at *8 (S.D. Ind. June 5, 2024) (no bailment where “Plaintiffs’ PII was not in
13 Defendants’ exclusive possession”); *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d
14 1154, 1177 (D. Minn. 2014) (no bailment of PII where defendant did not agree to return property
15 and “Plaintiffs allege that third parties stole the information, not that [defendant] wrongfully
16 retained that information”).

17 Plaintiffs’ attempt to plead a duty under the doctrine of negligence *per se* based on alleged
18 violations of the FTC Act or Nevada’s data privacy law, Nev. Rev. Stat. § 603A.210, also falls
19 short. To start with, the FTC Act “does not permit a private cause of action,” so “district courts do
20 not permit negligence *per se* claims to hinge on the [FTC Act].” *Baton v. Ledger SAS*, 2024 WL
21 3447511, at *40 (N.D. Cal. July 16, 2024). Plaintiffs likewise cannot rely on the Nevada state law,
22 because that law applies to “personal information of a resident of [Nevada] State,” Nev. Rev. Stat.
23 § 603A.210, and thus named Plaintiffs—none of whom are Nevada residents—are not within “the
24 class of persons whom the statute is intended to protect,” *Sanchez*, 125 Nev. at 828. Additionally,
25 “[t]o the extent Plaintiffs seek to rest their negligence *per se* on ‘similar state statutes,’ this is
26 insufficient to state a claim.” *Baton*, 2024 WL 3447511, at *40.

27 Finally, Plaintiffs’ suggestion that Caesars’ Privacy Policy creates a duty to prevent third
28 party conduct is misplaced, as the policy does not mention the risk of third party cyberattacks at

all. In fact, it warns that “Caesars cannot guarantee” that Plaintiffs’ data would be secure. CAC ¶ 239.

2. Plaintiffs Do Not Allege a Breach of Duty

Regardless of whether Caesars owed a duty to Plaintiffs, the Complaint does not specify any conduct that could constitute a breach of that duty.

To plausibly allege a breach, Plaintiffs cannot simply assert that unauthorized access of their PII occurred—they must allege facts sufficient to show how Caesars’ data security measures were inadequate. The Complaint summarizes a laundry list of recommended cybersecurity practices, CAC ¶¶ 253, 261-67, and then baldly concludes that Caesars must have failed to adhere to those practices simply because the breach occurred. *Id.* ¶ 268. But Plaintiffs do not allege which (if any) of these security practices Caesars allegedly failed to implement, or how any such alleged failure caused the Attack. More generally, federal courts have overwhelmingly rejected claims based on nothing more than the “implied premise that because data was hacked [Defendants’] protections must have been inadequate.” *Kuhns v. Scottrade, Inc.*, 868 F.3d 711, 717 (8th Cir. 2017); *see, also In re MCG Health Data Sec. Issue Litig.*, 2023 WL 3057428, at *4 (W.D. Wash. Mar. 27, 2023) (rejecting position “that, because there was a data breach, [defendant] did not implement adequate security”); *Griffey v. Magellan Health Inc.*, 562 F. Supp. 3d 34, 50 (D. Ariz. 2021) (“[T]he existence of an adequate data security infrastructure and two data breaches in a year are not mutually exclusive.”); *In re Equifax Inc. Sec. Litig.*, 357 F. Supp. 3d 1189, 1226 (N.D. Ga. 2019) (“[T]he occurrence of a data breach does not necessarily imply that a company’s data security is inadequate.”). Plaintiffs must offer “specific reasons explaining why [the company’s] data security was inadequate,” beyond just referring to various security standards. *Griffey*, 562 F. Supp. 3d at 50; *see also Anderson v. Kimpton Hotel & Rest. Grp., LLC*, 2019 WL 3753308, at *5 (N.D. Cal. Aug. 8, 2019) (dismissing statutory and common law claims because plaintiffs “fail[ed] to allege any facts in support of their conclusory assertion that” the defendant did not implement reasonable security protocols).

These cases persuasively acknowledge that a successful (criminal) cyber-attack, without more, does not plausibly plead negligence because “there is no such thing as perfect security, and

breaches can happen even when a company has taken every reasonable precaution.” Data Breaches and Identity Theft: Hearing Before the S. Comm. on Commerce, Sci., & Transp., 109th Cong. 6 (2005) (statement of Deborah Platt Majoras, Chairman, Federal Trade Commission); *see also* *Griffey*, 562 F. Supp. 3d at 50 (“[T]he existence of an adequate data security infrastructure and two data breaches in a year are not mutually exclusive.”). This is particularly true where, as here, Plaintiffs acknowledge that the attackers gained access to Caesars’ systems through a *third party vendor*, and not due to any vulnerabilities or deficiencies in Caesars own security systems. Permitting non-cognizable claims to proceed to discovery whenever plaintiffs allege that their data was impacted by a criminal cyberattack would effectively create a strict liability scheme for data privacy. This would undermine the very purpose of negligence law, which is intended to impose liability only based on departures from a “reasonable” standard of care that cause foreseeable harm.

Plaintiffs’ pleading failure is more than an oversight: it stems from the fundamental facts of the breach. As Plaintiffs acknowledge, the data breach resulted from “social engineering techniques” aimed at a *third-party* “IT support vendor,” and was perpetrated by a highly sophisticated cybercriminal group. ¶ 264-65. Setting aside their failure to plead any specific defect in Caesars’ security measures, Plaintiffs do not explain how the various frameworks and standards they identify are relevant to an attack initiated against an “outside” vendor, whose personnel was tricked by a sophisticated criminal into granting the hackers access. CAC ¶¶ 264-65. Without more, Plaintiffs do not plausibly allege that Caesars breached any duty of care.

3. Plaintiffs’ Alleged Damages Are Barred by the Economic Loss Doctrine

Nevada law provides “that unless there is personal injury or property damage, a plaintiff may not recover in negligence for economic losses.” *Terracon Consultants W., Inc. v. Mandalay Resort Grp.*, 125 Nev. 66, 87 (2009). This rule is based on Nevada’s policy recognizing “the need for useful commercial economic activity,” *id.*, and “protects parties from unlimited economic liability” that could otherwise arise from unintentional torts in commercial settings, *Halcrow, Inc. v. Eighth Jud. Dist. Ct.*, 129 Nev. 394, 399 (2013); *see Peri & Sons Farms, Inc. v. Jain Irr., Inc.*, 933 F. Supp. 2d 1279, 1284 (D. Nev. 2013) (observing “the premise that economic interests are

protected, if at all, by contract principles, rather than tort principles”).

Plaintiffs here do not adequately allege any noneconomic losses. To be sure, a minority of Plaintiffs do mention *some* noneconomic injuries such as alleged “anxiety.” *See, e.g.*, CAC ¶¶ 18, 60. But even if those alleged damages sufficed to establish standing (they do not), Nevada law does not recognize them for purposes of establishing compensable negligence damages, which “is a different question.” *Pruchnicki*, 845 F. App’x at 614. The allegations amount to no more than “‘naked assertions’ devoid of ‘further factual enhancement.’” *Iqbal*, 556 U.S. at 678 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007)). Such “unadorned, the-defendant-unlawfully-harmed-me accusation[s]” cannot survive Rule 8’s pleading standard. *Id.* If they did, any plaintiff would be able to thwart Nevada’s policy by surviving a motion to dismiss and potentially extracting substantial settlements on the basis of vague and unfounded assertions of injury. *See Terracon*, 125 Nev. at 87 (describing policy). The only alleged injuries that receive any factual enhancement in the CAC, by contrast, are clearly claimed economic injuries, including costs for credit services and purported benefit-of-the-bargain damages. *In re Zappos.com, Inc.*, 2013 WL 4830497, at *3 (D. Nev. Sept. 9, 2013) (economic loss doctrine barred simple negligence claim based on data breach where plaintiffs alleged similar economic injuries). Because recovery for such injuries is barred by the economic loss rule, Plaintiffs’ negligence claim should be dismissed.

E. Plaintiffs Do Not State an Implied Contract Claim

To state a claim for breach of an implied contract, Plaintiffs must show: “(1) the existence of a valid contract; (2) a breach by the defendant; and (3) damage as a result of the breach.” *Mizrahi v. Wells Fargo Home Mortg.*, 2010 WL 2521742, at *3 (D. Nev. June 16, 2010). Plaintiffs have not and cannot do so.

First, Plaintiffs fail to allege a contractual term that was allegedly breached. Plaintiffs claim that they entered into implied contracts with Caesars “under which Caesars agreed to adopt reasonable steps to protect their PII.” CAC ¶ 345. But they do not point to any specific promise Caesars made, or identify any other “specific term[] of the implied contracts.” *Griffey*, 562 F. Supp. 3d at 51. Earlier in the Complaint, Plaintiffs highlight a statement in Caesars’ Privacy Policy that Caesars “maintain[s] physical, electronic and organizational safeguards that reasonably and

appropriately protect against the loss, misuse and alteration of the information under our control.” CAC ¶ 239. But that language merely states that Caesars employs “reasonable” and “appropriate” safeguards, and cannot plausibly be read as a promise that those measures will be 100% effective at thwarting malicious criminal hacking attempts. *Id.* To the contrary, the Privacy Policy goes on to state that “Caesars cannot guarantee or warrant the security of any information you transmit” (*id.*)—and therefore cannot serve as the basis for a breach of contract claim. *See Kuhns*, 868 F.3d at 717 (“[Plaintiff] does not allege that Scottrade affirmatively promised that its customer data would not be hacked, and such a promise may not be plausibly implied.”); *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 610–11 (9th Cir. 2020) (holding that Facebook’s Privacy Policy was not a contract because it did “not outline shared commitments to which users must abide”); *Flores v. United Parcel Serv., Inc.*, 768 F. App’x 677, 679 (9th Cir. 2019) (affirming dismissal of contract claim where “documents ‘contain[] no promissory language’ that would oblige UPS to use a particular mode of transportation”). Plaintiffs’ implied contract claim therefore fails for the simple reason that they have not pled an implied contract as to data security.

Second, even if they had sufficiently pled the existence of an implied contract, Plaintiffs fail to allege any breach. Plaintiffs do not allege that the implied contract required perfect data security such that no breach could ever occur. Rather, Plaintiffs claim “Caesars breached its implied contracts . . . by failing to implement reasonable data security measures.” CAC ¶ 352. But Plaintiffs do not allege how Caesars violated this alleged promise other than the fact that the data breach occurred. As detailed above, the claim that a company “fail[ed] to implement reasonable data security measures” “does not assert more than the mere possibility of misconduct.” *Kuhns*, 868 F.3d at 717. Indeed, the “implied premise that because data was hacked [Caesars’] protections must have been inadequate is a naked assertion[] devoid of further factual enhancement that cannot survive a motion to dismiss.” *Id.* (citations omitted). Beyond that “naked assertion,” Plaintiffs’ “vague allegations do not establish how [Caesars] failed to take reasonable measures to protect customer’s data.” *Gardiner v. Walmart Inc.*, 2021 WL 2520103, at *6 (N.D. Cal. Mar. 5, 2021); *see also Razuki v. Caliber Home Loans, Inc.*, 2018 WL 2761818, at *3 (S.D. Cal. June 8, 2018).

1 *Third*, as stated above, Plaintiffs fail to show cognizable damages, which they must.
 2 *Pruchnicki*, 439 F. Supp. 3d at 1236. (dismissing implied contract claim in data breach context for
 3 lack of damages). Where (as here) Plaintiffs “do[] not allege any out-of-pocket expenses related
 4 to the underlying data breach” that were necessarily incurred, they cannot support the damages
 5 element of their contract claim. *Id.* at 1234; *see supra* at 9. Plaintiffs’ breach of implied contract
 6 claim fails for each of these independent reasons.

7 **F. Plaintiffs Do Not Plead a Viable Unjust Enrichment Claim**

8 To state an unjust enrichment claim, Plaintiffs must show: “(1) a benefit conferred on the
 9 defendant by the plaintiff; (2) appreciation of the benefit by the defendant; and (3) acceptance and
 10 retention of the benefit by the defendant (4) in circumstances where it would be inequitable to
 11 retain the benefit without payment.” *Ames v. Caesars Entm’t. Corp.*, 2019 WL 1441613, at *5 (D.
 12 Nev. Apr. 1, 2019) (citation omitted). Plaintiffs cannot make out an unjust enrichment claim here.

13 *First*, unjust enrichment is a form of equitable relief, which Plaintiffs cannot seek because
 14 they do not plead a lack of legal remedies. As the Ninth Circuit has held in *Sonner v. Premier*
 15 *Nutrition Corporation*, under federal law, plaintiffs cannot pursue equitable remedies unless they
 16 can show they lack an adequate remedy at law. 971 F.3d 834, 845 (9th Cir. 2020) (“[W]hen a plain,
 17 adequate, and complete remedy exists at law, we hold that federal courts rely on federal equitable
 18 principles before allowing equitable restitution in such circumstances.”). Unjust enrichment is
 19 equitable in nature. *H&H Pharm., LLC v. Chattem Chemicals, Inc.*, 2020 WL 376648, at *15 (D.
 20 Nev. Jan. 23, 2020). So too is the remedy of disgorgement, which Plaintiffs expressly seek. CAC
 21 ¶ 368; *see also JL Beverage Co., LLC v. Beam Inc.*, 2017 WL 5158661, at *2 (D. Nev. Nov. 7,
 22 2017) (“disgorgement is an equitable remedy”). Yet Plaintiffs make no allegation sufficient to
 23 show they lack an adequate remedy at law. To the contrary, Plaintiffs seek “monetary damages”
 24 and statutory damages for virtually all of their other claims, which are based on the *same conduct*
 25 underlying their putative unjust enrichment. Because Plaintiffs have not shown (and cannot show)
 26 they lack legal remedies, their unjust enrichment claims are barred by *Sonner*. *See, e.g., Sharma v.*
 27 *Volkswagen AG*, 524 F. Supp.3d 891, 909 (N.D. Cal. 2021) (“Because they have not shown that
 28 legal remedies are unavailable or inadequate as to either past or future injury, Plaintiffs’ CLRA,

UCL, and unjust enrichment claims must be dismissed.”)

Second, Plaintiffs fail to plead that they conferred any “benefit” on Caesars that was “unjustly” retained. Plaintiffs’ allegation that they paid “monetary consideration” for hotel reservations cannot suffice, as Plaintiffs do not claim that Caesars failed to provide a benefit in return (i.e., providing the hotel rooms). CAC ¶ 359. Plaintiffs alternatively suggest that Caesars profited in unspecified ways by simply receiving their PII. This theory requires that the information itself had “independent monetary value” that Caesars actually retained the benefits from. *In re Arthur J. Gallagher Data Breach Litig.*, 631 F. Supp. 3d 573, 592 (N.D. Ill. 2022); *see also In re Zappos.com*, 2013 4830497, at *5 (dismissing unjust enrichment claim in data breach case because customers did not “bestow[] any gratuitous benefit upon Defendant” by simply providing their PII). But Plaintiffs fail to allege that Caesars somehow sold or otherwise profited from the use of Plaintiffs’ PII. And while Plaintiffs allege that Caesars used their PII to “market[]” services to them (CAC ¶ 359), they do not allege that they were denied those services or that Caesars somehow profited from “marketing” alone. The unjust enrichment claim should be dismissed.

G. Plaintiffs’ Statutory Claims Fail on Numerous Grounds

Besides failing for standing, all of Plaintiffs’ statutory claims fail because: (1) the majority of the claims are grounded in fraud, but Plaintiffs do not plead any actionable misrepresentations or omissions (much less with the particularity required by Rule 9(b)); and (2) the claims based on deficient notice of the breach fail due to a lack of any harm cognizable under the statutes.

1. Plaintiffs’ Misrepresentation-Based Claims Are Uniformly Deficient (Counts IV, V, VI, IX, X, XI, XII, XIII, XV, XVI, XVIII)

Plaintiffs assert statutory claims alleging fraud and deceptive or unfair trade practices under nine different state laws. With few exceptions, these claims are all based on allegations of “consumer fraud” and must be pled with particularity under Rule 9(b). *See Urb. Outfitters, Inc. v. Dermody Operating Co., LLC*, 2022 WL 4134127, at *4 (D. Nev. Sept. 12, 2022) (applying Rule 9(b) to Nevada Consumer Fraud Act claim); *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124-25 (9th Cir. 2009) (California UCL’s fraudulent prong and CLRA); *Kahn v. Walmart Inc.*, 107 F.4th 585, 594 (7th Cir. 2024) (Illinois Consumer Fraud Act and Illinois Deceptive Trade Practices Act);

Himan v. Thor Indus., Inc., 2022 WL 683650, at *13 (N.D. Ind. Mar. 8, 2022) (Indiana Deceptive Consumer Sales Act claim); *Grady v. Progressive Direct Ins. Co.*, 643 F. Supp. 3d 929, 935 (D. Minn. 2022) (Minnesota Consumer Fraud Act); *Mekhail v. N. Mem'l Health Care*, 2024 WL 1332260, at *7 (D. Minn. Mar. 28, 2024) (Minnesota Uniform Deceptive Trade Practices Act); *Griffey*, 562 F. Supp. 3d at 54 (Pennsylvania Unfair Trade Practices And Consumer Protection Law); *Houston v. DTN Operating Co., LLC*, 2017 WL 4653246, at *8 (E.D. Tex. Oct. 17, 2017) (Texas Deceptive Trade Practices-Consumer Protection Act); *Nahigian v. Juno Loudoun, LLC*, 684 F. Supp. 2d 731, 741 (E.D. Va. 2010) (Virginia Consumer Protection Act).

Plaintiffs base their fraud and deceptive practices claims on two primary sets of allegations: (i) alleged misrepresentations or omissions by Caesars concerning its data security practices; and (ii) alleged “deceptive” or “unfair” business practices based on an asserted “failure to implement reasonable security practices and procedures.” In both cases⁹, the allegations are subject to Rule 9(b), which requires Plaintiffs to “state with particularity the circumstances constituting fraud” including the “time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations.” *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (citation omitted). When an entire claim is “grounded in fraud,” then failure to plead supporting allegations with particularity demands dismissing the claim in full. *Vess*, 317 F.3d at 1107. Plaintiffs’ allegations fall far short of this standard.

Misrepresentations and Omissions. In vague and conclusory fashion, Plaintiffs allege that Caesars misled them about Caesars’ “data security safeguards,” CAC ¶ 239. But “Plaintiffs do not allege any details about when [Caesars] made [any] misrepresentation[s], or the manner in which [Caesars] made these misrepresentations to plaintiffs.” *Jackson v. Anheuser-Busch InBev SA/NV, LLC*, 2021 WL 3666312, at *17 (S.D. Fla. Aug. 18, 2021). The CAC’s statutory counts

⁹ Plaintiffs’ allegations of “unfair” practices stem from the same facts underlying their deceptive and fraudulent practices claims. *Compare*, e.g., CAC ¶ 478 (alleging Caesars’ “fail[ure] to comply with common law and statutory duties” and “fail[ure] to implement and maintain reasonable security and privacy measures”) *with id.* ¶ 478 (alleging that Caesars “misrepresent[ed] that it would comply with common law and statutory duties” and “misrepresent[ed]” that it would implement “reasonable security measures”). Both sets of allegations are therefore “grounded in fraud” and are subject to Rule 9(b). *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103 (9th Cir. 2003).

merely assert that Caesars “misrepresent[ed] that it would protect the privacy and confidentiality” of Plaintiffs’ PII and “misrepresent[ed] that it would comply with common law and statutory duties pertaining to the security and privacy” of Plaintiffs’ information—but Plaintiffs do not specify what statement by Caesars supposedly made this misrepresentation. CAC ¶¶ 401-402, 468, 478, 487, 508, 519, 529, 549, 578. These are simply “conclusory allegations of wrongdoing that are too vague to state a valid claim for fraud under the heightened pleading standards.” *Mauer v. Am. Home Mortg. Acceptance, Inc.*, 2011 WL 6752631, at *4 (D. Nev. Dec. 23, 2011).

To the extent that Plaintiffs rely on alleged representations made in Caesars’ Privacy Policy, *see* CAC ¶ 239, not only do Plaintiffs fail to mention any specific Privacy Policy provision in their statutory counts, they also nowhere allege that they actually read those policies prior to engaging in any transaction with Caesars. This is inadequate. *See, e.g., In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *37 (N.D. Cal. May 27, 2016) (rejecting fraud claim based on privacy policy where no plaintiff “allege[s] that they saw, read, or—for that matter—even knew about Anthem’s privacy policies prior to the data breach.”). And it is even more inadequate for statutes that demand actual reliance—which include the Nevada Consumer Fraud Act (Count IV), California UCL (Count V), Indiana Deceptive Consumer Sales Act (Count XI), Pennsylvania Unfair Trade Practices and Consumer Protection Law (Count XV), Texas Deceptive Trade Practices Act (Count XVI), and Virginia Consumer Protection Act (Count XVIII). *See In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 998 (S.D. Cal. 2014) (rejecting reliance where the Plaintiffs engaged in the transaction before seeing the policy); *In re Rutter’s Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 542 (M.D. Pa. 2021) (finding general allegations pertaining to the privacy policy too conclusory to show reliance as required by Pennsylvania CPA).¹⁰

¹⁰ *See also Guerra v. Dematic Corp.*, 2020 WL 5995496, at *2 (D. Nev. Oct. 8, 2020) (Count IV); *Ehrlich v. BMW of N. Am., LLC*, 801 F.Supp.2d 908, 919 (C.D. Cal. 2010) (Count V); *Gordon v. Finch*, 2023 WL 3496427, at *8 (N.D. Ind. May 17, 2023) (Count XI); *Cruz v. Andrews Restoration, Inc.*, 364 S.W.3d 817, 823 (Tex. 2012) (Count XVI); *Orr v. Keystone RV Co.*, 2024 WL 2883510, at *5 (E.D. Va. June 7, 2024) (Count XVIII).

Plaintiffs cannot salvage their fraud claims by predicated them on an omissions theory. At the outset, Plaintiffs have failed to identify any specific facts about Caesars’ data security measures that it allegedly failed to disclose. Mere allegations that a defendant failed to disclose that its security systems were not 100% secure or that it could not guarantee protection against a data breach are insufficient as a matter of law. And any such claim would contradict the Privacy Policy in any event, which disclosed only that Caesars employed “reasonabl[e] and “appropriat[e]” security measures and—in the very next sentence—warned that “Caesars cannot guarantee or warrant the security of any [consumer] information” transmitted to Caesars. CAC ¶ 239. *See, e.g., Yuille v. Uphold HQ Inc.*, 686 F. Supp. 3d 323, 347-48 (S.D.N.Y. 2023) (dismissing claim where reframing statements as omissions “could not have communicated the impression that [the] platform was so secure that no hackers, no matter how talented, could penetrate [the] platform”); *In re Rutter’s*, 511 F. Supp. 3d at 542 (determining that the omission-based claims could not be squared away with allegations in the complaint about similar misrepresentations).

In any event, any omission-based theory fails because Plaintiffs do not plausibly allege that Caesars had knowledge of any security deficiencies or a duty to disclose them. Several of Plaintiffs’ statutory claims require actual knowledge of the fact omitted¹¹, while others will find “fraud by omission” only if there was a “duty to disclose” a material, omitted fact.¹² The Complaint alleges in a conclusory fashion that Caesars “knew or should have known” of the risk of data breaches to the hotel industry, *see* CAC ¶ 243, and then later say Caesars “knew or should have known” that its “data security practices were deficient,” *see, e.g.,* CAC ¶¶ 374, 394, 430. Not only are these allegations untethered to the nature of the breach—i.e., in which *a third-party vendor* allowed the attacker into Caesars’ network—but Plaintiffs fail to allege any facts showing that Caesars *knowingly* failed to disclose anything to Plaintiffs in an attempt to mislead them. As to a

¹¹ Nev. Rev. Stat. § 598.0923(2) (“knowingly ... (2) Fails to disclose) (Count IV); *Thor Indus.*, 2022 WL 683650, at *14 (Count XI); *eFinanzas, S.A.S. v. Roy*, 2024 WL 1705471, at *5 (S.D. Tex. Apr. 4, 2024) (Count XV); *Belmont v. MB Inv. Partners, Inc.*, 708 F.3d 470, 498 (3d Cir. 2013) (Count XVI); *Guy v. Tidewater Inv. Props.*, 41 Va. Cir. 218 (1996) (Count XVIII).

¹² *Daugherty v. Am. Honda Motor Co.*, 144 Cal. App. 4th 824, 835, (2006) (Count V); *Thor Indus.*, 2022 WL 683650, at *14 (Count XI); *Song v. Champion Petfoods USA, Inc.*, 2020 WL 7624861, at *11 (D. Minn. Dec. 22, 2020), *aff’d*, 27 F.4th 1339 (8th Cir. 2022) (Count XII).

1 duty to disclose, no such duty arises here, where the only alleged duty is predicated on an arms-
 2 length, economic “relationship between Caesars and the Plaintiff[s],” *e.g.*, CAC ¶ 497. *See In re*
 3 *Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp. 3d 1295, 1337 (N.D. Ga. 2019) (“In
 4 the absence of a confidential relationship, no duty to disclose exists when parties are engaged in
 5 arm’s-length business negotiations; in fact, an arm’s length relationship by its nature excludes a
 6 confidential relationship.”); *Song*, 2020 WL 7624861, at *11 (“Minnesota courts almost never find
 7 that one party’s ‘special knowledge’ triggers a duty to disclose.”).

8 **Reasonable Security Measures.** Plaintiffs also attempt to assert “deceptive” or “unfair”
 9 trade practices based on bare allegations that Caesars “failed to implement and maintain reasonable
 10 security” measures or to “identify and remediate” alleged security risks. *See* CAC ¶¶ 330, 387-
 11 388, 398-399, 468, 478, 487, 508, 518, 529, 549, 578. These allegations are deficient as a matter
 12 of law, whether measured against Rule 9(b) or Rule 8’s plausibility standard. Plaintiffs cite to
 13 various industry security standards (CAC ¶¶ 253, 263, 266), but do not allege that Caesars
 14 represented its compliance with those specific standards or that Caesars actually failed to meet
 15 them. *See Maag v. U.S. Bank, Nat’l Ass’n*, 2021 WL 5605278, at *2 (S.D. Cal. Apr. 8, 2021)
 16 (holding that bare allegations of failure to use “reasonable security procedures” or “effectively
 17 monitor its systems for security vulnerabilities” are insufficient). Setting aside their conclusory
 18 pleading, Plaintiffs do not allege any specific failure by Caesars to implement reasonable security
 19 measures. Instead, their “deceptive” and “unfair” practices theories boil down to this: the data
 20 breach happened; therefore, Caesars necessarily failed to employ adequate security measures,
 21 knew it did not employ adequate security measures, and intentionally withheld that information
 22 from customers. For good reason, that is not the law. *See Kuhns*, 868 F.3d at 717 (“The implied
 23 premise that because data was hacked Scottrade’s protections must have been inadequate is a naked
 24 assertion devoid of further factual enhancement that cannot survive a motion to dismiss.” (cleaned
 25 up)); *Griffey*, 562 F. Supp. 3d at 54–55 (holding that the plaintiff’s “Pennsylvania claim fails
 26 because [plaintiff] has not explained with any specificity how [defendant’s] data security was
 27 inadequate beyond pointing to the fact that a security breach happened.”).

2. Plaintiffs’ Data Breach Notification Statute Claims Fail to Allege Cognizable Harm (Counts VII, VIII, XVII)

Plaintiffs attempt to plead claims based on California (Count VII), Illinois (Count VIII), and Virginia (Count XVII) statutes mandating timely disclosure of certain data security incidents. *See* Cal. Civ. Code § 1798.82(a) (requiring disclosure “without reasonable delay”); 815 Ill. Comp. Stat. § 530/10(a) (same); Va. Code Ann. §§ 18.2-186.6 (same). But Plaintiffs cannot show that Caesars unreasonably delayed disclosing the Attack, or that Plaintiffs suffered harm from any purported delay.

Instead, Plaintiffs’ own allegations show that Caesars met its disclosure obligations. Upon discovering and containing the Attack, Caesars promptly disclosed it via a Form 8-K and customer-facing public website on September 14, 2023, only a few weeks after the Attack began. *See* CAC ¶¶ 228-229. The website contained directions for customers to accept Caesars’ credit monitoring offer, *id.*, and Caesars’ announcement generated extensive press coverage surrounding the incident—through which several Plaintiffs, including Plaintiff Rodriguez, first learned about the breach. *See, e.g.,* CAC ¶ 37; *see also* ECF 1 ¶¶ 1, n1, 42. In addition, just a few weeks later, Caesars followed up with individual notices, *see, e.g.,* CAC ¶ 26, after undertaking substantial efforts to identify potentially affected individuals and their contact information. Caesars’ notification efforts were not only reasonable, they were exemplary—and Plaintiffs do not plausibly allege any facts to show otherwise. *Compare, e.g., Razuki v. Caliber Home Loans, Inc.*, 2018 WL 6018361, at *2 (S.D. Cal. Nov. 15, 2018) (dismissing claim under Cal. Civ. Code § 1798.82(a) because notice issued five months after incident was not “unreasonabl[y] delay[ed]”).

In any case, because these statutes only regulate the timing of the notice, “Plaintiffs must allege incremental harm suffered as a result of [any] alleged delay in notification,” as opposed to harm from the incident itself. *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 613 F.Supp.3d 1284, 1300 (S.D. Cal. May 7, 2020); *see also Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *6-7 (S.D. Cal. Nov. 3, 2016) (dismissing California CRA claim where it was “entirely unclear how any of the injuries identified by Plaintiff ha[d] been caused or compounded by Defendants’ alleged failure to promptly notify Plaintiff”); *Fox v. Iowa*

1 *Health Sys.*, 399 F.Supp.3d 780, 801 (W.D. Wisc. 2019) (dismissing claim under Illinois statute
 2 where plaintiffs “failed to allege any damages that were caused by the timing of the notifications”).
 3 Plaintiffs offer nothing more than a conclusory allegation that the alleged delay in sending
 4 “individual notice” “exacerbated the harm to Class Members by preventing them from taking steps
 5 to mitigate” the effects of the breach. CAC ¶ 230.¹³ But Plaintiffs do not allege any *facts* showing
 6 that any purported delay prevented them from taking any specific mitigating action, or that they
 7 suffered any actual, incremental harm in the short period before Caesars sent individual notice
 8 letters. Because Plaintiffs fail to allege any damages or incremental injury from the alleged delay
 9 in notification, these delayed notice claims are properly dismissed as a matter of law.

10 **H. Plaintiffs’ Individual Statutory Claims Fail for Additional Reasons**

11 **1. The Texas Deceptive Practices Act Claim Must Be Voluntarily** 12 **Dismissed, or the Entire Case Must Be Abated**

13 As a threshold matter, Plaintiff Huddleston did not comply with the pre-suit “written
 14 notice” requirements of the Texas DTPA. Section 17.505 of the statute mandates that:

15 As a prerequisite to filing a suit seeking damages under [the DTPA] against any person, a
 16 consumer shall give written notice to the person *at least 60 days before filing the suit*
 17 advising the person in *reasonable detail* of the *consumer’s specific complaint and the*
 18 *amount of economic damages*, damages for mental anguish, and expenses, including
 attorneys’ fees, if any, reasonably incurred by the consumer in asserting the claim against
 defendant.

19 Tex. Bus. & Com. Code § 17.505(a) (emphasis added). Adequate pre-suit notice is key to the
 20 DTPA’s statutory scheme, which encourages informal resolution of disputes and permits
 21 defendants to recover appropriate sanctions when a claim is initiated without notice. *See Hines v.*
 22 *Hash*, 843 S.W.2d 464, 469-70 (Tex. 1992). Not only must notice be timely, any claimed damages
 23 and expenses must be described with “reasonable detail” to facilitate offers of settlement and
 24 associated defenses that are available under the statute. Tex. Bus. & Com. Code § 17.505(a). And

25
 26 ¹³ Plaintiffs assert that Caesars did not send “individual notice” letters until early October 2023,
 27 but ignore the fact that Caesars publicly announced the breach—and the fact that it affected all
 28 registered Caesars Rewards members—several weeks earlier, on September 14, 2024. CAC ¶ 228.
 That notification advised members on steps they could take to mitigate the potential impacts of the
 breach, and informed members of Caesars’ offer of complimentary credit monitoring and
 protection services. *See* Form 8-K at 2.

1 where a defendant denies receiving notice, “the plaintiff must prove that he provided it.” *Winkle*
 2 *Chevy-Olds-Pontiac, Inc. v. Condon*, 830 S.W.2d 740, 745 (Tex. App. 1992).

3 Here, Plaintiff Huddleston has disregarded both the timing and content requirements of the
 4 notice provision. He alleges in conclusory fashion that he complied with the statute’s notice
 5 requirement (see CAC ¶ 560), based solely on the fact that other complaints were filed earlier
 6 relating to the breach. But Huddleston did not provide pre-suit notice of *his* claim—he is a new
 7 plaintiff in the Consolidated Complaint, and the first to assert a Texas DTPA claim against Caesars
 8 relating to the breach—much less provide notice and “reasonable detail” of the specific amount of
 9 “economic damages” and expenses he is seeking under the statute. Even in the Complaint—which
 10 cannot substitute for the requisite pre-suit notice under Section 17.505—Plaintiff Huddleston
 11 makes no effort to quantify his alleged economic damages, or even make a claim that he suffered
 12 out-of-pocket losses at all. CAC ¶¶ 189-190. *See Clark v. Wells Fargo Home Mortg.*, 2014 WL
 13 5297723, at *2 (N.D. Tex. Oct. 16, 2014) (finding notice insufficient for failing to specify
 14 economic damages).

15 Where, as here, a plaintiff fails to provide the mandatory notice under the DTPA, the proper
 16 remedy is to abate the entire suit for the statutory period so that the intended pre-suit negotiations
 17 can occur. *See Daniels v. AETC II Privatized Housing LLC*, 2020 WL 6789336, at *4-5 (W.D. Tex.
 18 Jan. 6, 2020) (finding that the entire suit should be abated for the statutory period if the plaintiff
 19 fails to meet statutory notice requirements); *Pierce v. N. Dall. Honey Co.*, 2020 WL 1047903, at
 20 *5 (N.D. Tex. Mar. 3, 2020) (“The Fifth Circuit and Texas Supreme Court have required abating
 21 the action until th[e] statutory requirement is met”); *Patel v. Holiday Hosp. Franchising, Inc.*, 172
 22 F. Supp. 2d 821, 826 (N.D. Tex. 2001) (“[D]efendants are entitled to have this action held in
 23 abeyance until plaintiffs comply with the DTPA’s notice requirements.”). Because the mandatory
 24 pre-suit notice was not provided, Plaintiffs must either voluntarily dismiss this claim, or this Court
 25 should abate the entire lawsuit under Section 17.505 until the statutory written notice is provided.

26 **2. The Nevada Consumer Fraud Act Claim Fails for Additional Reasons**

27 To state a claim under the Nevada Consumer Fraud Act, Plaintiffs must show “(1) an act
 28 of consumer fraud by the defendant (2) caused (3) damage to the plaintiff.” *Picus v. Wal-Mart*

1 *Stores, Inc.*, 256 F.R.D. 651, 658 (D. Nev. 2009). Plaintiffs’ Nevada claim—brought on behalf of
 2 all named Plaintiffs—is based entirely on an omission theory. CAC ¶ 371 (alleging that Caesars
 3 “failed to disclose the material fact that its data security practices were deficient”). “For a mere
 4 omission to constitute actionable fraud” under Nevada law, however, Plaintiffs “must first
 5 demonstrate that [Caesars] had a duty to disclose the fact at issue.” *Soffer v. Five Mile Cap.*
 6 *Partners, LLC*, 2013 WL 638832, at *10 (D. Nev. Feb. 19, 2013); *see also Taddeo v. Taddeo*, 2011
 7 WL 4074433, at *6 n.3 (D. Nev. Sept. 13, 2011) (same). Plaintiffs, however, plead no facts
 8 establishing any duty to disclose on the part of Caesars, such as a “fiduciary relationship.” *Soffer*,
 9 2013 WL 638832, at *10 (dismissing Nevada CFA claim based on lack of duty to disclose). To
 10 the extent Plaintiffs are claiming that a duty arose due to their customer relationship with Caesars,
 11 the majority of Plaintiffs only claim to have “gambled” at Caesars properties or online and joined
 12 the Rewards program to earn associated perks. And even as to those who claim to have stayed at
 13 a Caesars property, “no Nevada case law . . . recognizes a fiduciary relationship between” a hotel
 14 and its guests. *See id.*; *see also Equifax*, 362 F. Supp. 3d at 1337 (dismissing Nevada Consumer
 15 Fraud Act claim predicated on omissions theory: “In the absence of a confidential relationship, no
 16 duty to disclose exists when parties are engaged in arm’s-length business negotiations; in fact, an
 17 arm’s length relationship by its nature excludes a confidential relationship.”).

18 Plaintiffs’ secondary theory is that Caesars’ alleged violations of other state and federal
 19 statutes also establishes a claim under the Nevada CFA. Not so. To base a Nevada CFA claim on
 20 the violation of another statute, Plaintiffs must “plead with particularity how the facts of this case
 21 pertain to that specific statute.” *See Baba v. Hewlett-Packard Co.*, 2010 WL2486353, at *6 (N.D.
 22 Cal. June 16, 2010). Plaintiffs first claim that Caesars violated Nev. Rev. Stat. § 603A.210(1),
 23 which requires businesses to “implement and maintain reasonable security measures” to protect
 24 the PII of Nevada residents in their possession. CAC ¶ 373. But that statute applies only to Nevada
 25 residents, and none of the Plaintiffs reside in Nevada. Nev. Rev. Stat. § 603A.210(1) (coverage
 26 limited to “personal information of a *resident of this State*”) (emphasis added).

27 Plaintiffs next allege that “Caesars breached other state statutes as alleged herein.” CAC ¶
 28 374. But for the reasons set forth elsewhere herein, Plaintiffs have not and cannot allege a violation

1 of those statutes.

2 Plaintiffs finally claim that Caesars violated the FTC Act, but their vague and conclusory
3 references to that statute miss the mark. CAC ¶ 375. Plaintiffs fail to plead specific facts concerning
4 how Caesars “knew or should have known that its data security practices were deficient,” how it
5 “violated the FTC Act,” or how it “failed to adhere to the FTC’s data security guidance.” *Id.* For
6 example, Plaintiffs do not say what guidance Caesars failed to adhere to, how Caesars failed to
7 adhere to it, how the alleged failure resulted in a social engineering attack on Caesars’ third-party
8 vendor, and how the alleged failures harmed Plaintiffs. This is the type of conclusory allegation
9 prohibited by *Twombly* and *Iqbal*. Indeed, allowing Plaintiffs’ deficient pleading to go forward
10 here would mean every business victimized by a data breach would be deemed to have violated
11 the FTC Act, as virtually every industry has been the “target of sophisticated cyberattacks.” CAC
12 ¶ 375. That plainly is not the law.

13 3. Plaintiffs’ California Statutory Claims Fail

14 The California Plaintiffs’ claims under California’s Unfair Competition Law (“UCL”) and
15 the Consumers Legal Remedies Act (“CLRA”) (Counts V-VI) additionally fail for lack of statutory
16 standing and failure to state a claim.

17 a. Plaintiffs Lack Statutory Standing Under the UCL and CLRA

18 **No Economic Injury.** Standing under the UCL and CLRA is “substantially narrower” than
19 Article III standing, *Kwikset Corp. v. Super. Ct.*, 51 Cal.4th 310, 324 (2011), with stringent
20 economic injury and causation requirements. *See Sony*, 903 F.Supp.2d at 965; *Pirozzi v. Apple,*
21 *Inc.*, 966 F.Supp.2d 909, 919 (N.D. Cal. 2013). To meet these requirements, a plaintiff must
22 establish “lost money or property” (UCL) or “economic injury” (CLRA). *Hinojos v. Kohl’s Corp.*,
23 718 F.3d 1098, 1104 (9th Cir. 2013); *see also Reid v. Johnson & Johnson*, 780 F.3d 952, 958 (9th
24 Cir. 2015) (“To establish standing to bring a claim under [the UCL and CLRA], plaintiffs must
25 meet an economic injury-in-fact requirement.”).

26 Plaintiffs’ allegations fall short on both fronts. Plaintiffs rely on a laundry list of purported
27 injuries, including “lost time and opportunity costs,” “loss of benefit of the bargain,” “increased
28 risk of identity theft and fraud,” and “daily fear and anxiety,” *e.g.*, CAC ¶¶ 18, 29, 39, but none

amount to cognizable economic harm. *See, e.g., Gardiner*, 2021 WL 2520103, at *6 (rejecting “benefit of the bargain” theory of economic damages under UCL); *Pruchnicki*, 439 F.Supp.3d at 1232 (increased risk of fraud and identity theft is not an economic injury); *Kuhns*, 868 F.3d at 718 (lawsuits must “be based on more than allegations of worry”). Plaintiffs further allege that they “lost money or property” through the “loss of value” in their PII (CAC ¶ 410), but they do not ascribe any value to their information, and courts have repeatedly found that the “loss of [plaintiffs’] personal information” is not “economic loss” for [UCL] standing purposes.” *Flores-Mendez v. Zoosk, Inc.*, 2021 WL 4553772, at *2-3 (N.D. Cal. Oct. 5, 2021); *see also Swarts v. Home Depot, Inc.*, 689 F.Supp.3d 732, 748 (N.D. Cal. 2023) (“Numerous courts have held that disclosure of personal information alone does not constitute economic or property loss sufficient to establish UCL standing, unless the plaintiff provides specific allegations regarding the value of the information”); *Gonzales v. Uber Techs., Inc.*, 305 F.Supp.3d 1078, 1093 (N.D. Cal. 2018) (“[T]he sharing of names, user IDs, location and other personal information does not constitute lost money or property for UCL standing purposes.”).

Finally, the California Plaintiffs individually make vague allegations of “unauthorized charges,” “late fees . . . for fraudulent” charges, and “nominal and statutory damages.” CAC ¶¶ 18, 29, 39. But Plaintiffs do not specify anything about the nature of these charges, plausibly tie them to the Attack, or claim that any of the charges were unreimbursed. And while Plaintiffs Gill and Hylton allege that they purchased credit monitoring services, CAC ¶¶ 17, 27, they fail to show that their expenses were “necessary” given Caesars’ offer of free “credit monitoring.” *Falkenberg v. Alere Home Monitoring, Inc.*, 2014 WL 5020431, at *4 (N.D. Cal. Oct. 7, 2014).¹⁴ Plaintiffs thus lack standing to sue under the UCL and CLRA.

No Causation. To the extent Plaintiffs’ California statutory claims are based on a deception theory, Plaintiffs must also allege with particularity their actual reliance on any misrepresentation or omission. *See Moore v. Mars Petcare US, Inc.*, 966 F.3d 1007, 1020 (9th Cir.

¹⁴ Plaintiff Hylton alleges she was denied enrollment in Caesars’ free credit monitoring services, but fails to plead any facts to substantiate that claim. In any event, Plaintiff Hylton admits she had been paying for credit monitoring services *before* the Attack and “continued to pay for this service” after the breach occurred, CAC ¶ 27, meaning such expenses were wholly unrelated to the breach.

2020) (UCL); *Davidson v. Apple, Inc.*, 2017 WL 976048, at *9 (N.D. Cal. Mar. 14, 2017) (CLRA and UCL); *see also Maxwell v. Unilever United States, Inc.*, 2014 WL 4275712, at *4 (N.D. Cal. Aug. 28, 2014) (actual reliance required under UCL “unlawful” and “unfair” prongs where “predicate unlawfulness is misrepresentation and deception”) (collecting cases).

Plaintiffs allege they “relied on Caesars’ policies and promises to implement sufficient measures to protect [their] PII and privacy rights.” CAC ¶¶ 21, 32, 42. But their “vague allegations do not establish *how* [the company] failed to take reasonable measures to protect customer’s [sic] data.” *Gardiner*, 2021 WL 2520103, at *6 (emphasis added). In addition, Plaintiffs never plead that they “actually read” Caesars’ Security policy, *Williams v. Apple, Inc.*, 449 F.Supp.3d 892, 912-13 (N.D. Cal. 2020), or that this policy was a “substantial factor[]” in their decision to provide their PII to Caesars, *In re iPhone App. Litig.*, 6 F.Supp.3d 1004, 1019-20 (N.D. Cal. 2013). In other words, Plaintiffs show no reliance on Caesars’ policies, because these policies never prompted Plaintiffs to provide their PII. This is fatal to Plaintiffs’ standing under the UCL and CLRA.

b. Plaintiffs’ UCL Claim Fails on Several Other Grounds

To state a claim under the UCL, California Plaintiffs must show an “unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising.” *Kearns*, 567 F. 3d at 1127 (“Each prong of the UCL is a separate and distinct theory of liability.”). Plaintiffs fail to do so.

First, Plaintiffs’ claim should be dismissed because they do not plausibly plead that they lack an adequate remedy at law. As the Ninth Circuit reaffirmed in *Sonner*, claims for equitable relief, such as restitution under the UCL, are proper only where a plaintiff lacks an adequate legal remedy. *See* 971 F.3d at 844; *see also Guzman v. Polaris Indus. Inc.*, 49 F.4th 1308, 1313-15 (9th Cir. 2022) (“district court lacked equitable jurisdiction to hear” UCL claim given that plaintiff had “an adequate legal remedy”). As detailed above, Plaintiffs seek “monetary damages” and statutory damages for virtually all of their other claims that are based on the *same conduct* underlying their UCL claim, without alleging that they lack an adequate remedy at law. It follows that the UCL claim should be dismissed. *See, e.g., Brickfire LLC v. Aetna Life Ins. Co.*, 2024 WL 1121007, at *6 (C.D. Cal. Feb. 16, 2024) (dismissing UCL claim under *Sonner*); *Hamm v. Mercedes-Benz*

1 *USA, LLC*, 2022 WL 913192, at *3-4 (N.D. Cal. Mar. 29, 2022) (same); *see supra* § IV.F.

2 *Second*, as to “unlawful” conduct, the California Plaintiffs cite to the CCRA, the CLRA,
3 and the FTC Act. CAC ¶ 392. The California Plaintiffs, however, fail to state violations of any of
4 those laws for the reasons stated elsewhere herein.

5 *Third*, Plaintiffs have no claim under the fraudulent prong because, in addition to the failure
6 to allege any actionable misrepresentation or omission (*see supra* § IV.G.1), no reasonable
7 consumer would be deceived by Caesars’ alleged misrepresentations about its security measures.
8 *See Williams v. Gerber Prods, Co.*, 552 F.3d 934, 938 (9th Cir. 2008) (Plaintiffs’ UCL claims
9 predicated on alleged misrepresentations “are governed by the reasonable consumer test,” whereby
10 a plaintiff must show “members of the public are likely to be deceived” (quotation marks and
11 citation omitted)); *Ebner v. Fresh, Inc.*, 838 F.3d 958, 965 (9th Cir. 2016) (To state a UCL
12 fraudulent claim, a plaintiff must allege “more than a mere possibility that [a representation] might
13 conceivably be misunderstood by some few customers viewing it in an unreasonable manner”;
14 rather, such plaintiff must allege facts showing “a probability that a significant portion of the
15 general consuming public...acting reasonably in the circumstances, could be misled.” (quotation
16 marks and citation omitted)).

17 As noted, Caesars explicitly states in its Privacy Policy that it “cannot guarantee or warrant
18 the security of any information [a customer] transmit[s] on or through a website or mobile app,
19 and [a customer] do[es] so at [their] own risk.” CAC ¶ 239. As this disclaimer indicates, reasonable
20 protection does not mean absolute protection—let alone protection against “social engineering”
21 attacks on Caesars’ third-party vendors. And Plaintiffs allege no facts showing that Caesars made
22 any representation to the contrary. Because Caesars “truthfully and clearly disclose[d] an alleged
23 misrepresentation or omission, [Caesars] cannot plausibly state a claim for relief” under either the
24 UCL or CLRA. *Hammerling v. Google, LLC*, 615 F.Supp.3d 1069, 1082 (N.D. Cal. 2022) (citing
25 *Dinan v. Sandisk LLC*, 2019 WL 2327923, at *2 (N.D. Cal. May, 31, 2019)).

26 *Finally*, Plaintiffs also do not adequately plead “unfair” conduct under either test used by
27 the courts, which require the challenged conduct to be either (i) “immoral, unethical, oppressive,
28 unscrupulous, or substantially injurious to consumers,” or (ii) “tethered to specific constitutional,

statutory, or regulatory provisions.” *Bardin v. DaimlerChrysler Corp.*, 136 Cal.App.4th 1255, 1260–61 (2006). Plaintiffs do not allege why Caesars’ purportedly unfair practices—generically identified as failing to “implement and maintain reasonable security measures” (CAC ¶ 389)—amount to “unethical, oppressive, [and/or] substantially injurious” conduct, particularly where (as here) Caesars disclosed that it could not guarantee perfect security, and the Attack occurred as a result of a social engineering attack on a third-party vendor. *See, e.g., Hodsdon v. Mars, Inc.*, 891 F.3d 857, 867 (9th Cir. 2018) (dismissing UCL unfairness claim where the alleged “failure to disclose” any additional information that the defendant “had no duty to disclose in the first place is not substantially injurious, immoral, or unethical”); *see also Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1170 (9th Cir. 2012). Nor do Plaintiffs even attempt to plead that Caesars violated any specific “constitutional or statutory provision . . . or a regulation carrying out statutory policy.” *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal.4th 163, 185 (1999).

c. Plaintiffs’ CLRA Claim Fails on Additional Grounds

Under the CLRA, Plaintiffs must plausibly allege reliance. *See Ehrlich*, 801 F.Supp.2d at 919; *Buckland v. Threshold Enters., Ltd.*, 155 Cal.App.4th 798, 810 (2007) (“In view of Caro, plaintiffs asserting CLRA claims sounding in fraud must establish that they actually relied on the relevant representations or omissions.” (citation omitted)) (disapproved of on other grounds by *Kwikset Corp.*, 51 Cal.4th at 337). For the reasons discussed above, Plaintiffs have failed to do so.

A CLRA claim also requires Plaintiffs to show that Caesars engaged in “unfair or deceptive acts or practices” that cause a “reasonable consumer” to be deceived by the defendant’s actions. *See Ebner*, 838 F.3d at 965 (describing same “reasonable consumer” test under the CLRA). In this regard, Plaintiffs’ CLRA claim is insufficiently pled for the same reason as the UCL fraud prong.

4. The Pennsylvania Unfair Trade Practice and Consumer Protection Law Claim Fails

Plaintiffs Blair Smith and Katz plead no facts to establish “any ascertainable loss of money or property,” as required by the Pennsylvania UTPCPL. *See Weinberg v. Sun Co., Inc.*, 565 Pa. 612, 617 (2001); *Benner v. Bank of America, N.A.*, 917 F.Supp.2d 338, 360 (E.D. Pa. 2013) (to

1 allege an ascertainable loss, the plaintiff “must be able to point to money or property that he would
 2 have had but for the defendant’s fraudulent actions”). To state a claim under the UTPCPL,
 3 “damages cannot be speculative,” *Jarzyna v. Home Props., L.P.*, 185 F. Supp. 3d 612, 626 (E.D.
 4 Pa. 2016), and general allegations that a plaintiff has suffered “emotional distress” are not
 5 sufficient. *Riviello v. Chase Bank USA, N.A.*, 2020 WL 1129956, at *4 (M.D. Pa. Mar. 4, 2020).
 6 None of the general categories of injuries alleged by the Pennsylvania Plaintiffs—consisting
 7 primarily of vague allegations concerning the “loss of ... PII,” “invasion of privacy,” “risk of
 8 identity theft,” and “anxiety” due to the breach—qualifies as an ascertainable loss. *See* CAC ¶¶
 9 170, 179. And while Plaintiff Katz alleges that there were “fraudulent transactions made on his
 10 credit card,” CAC ¶ 180, he fails to allege that these charges unreimbursed, or plausibly connect
 11 the attempted charges to the breach, given that bank or payment card information was not
 12 impacted.

13 In addition, a plaintiff under the UTPCPL must plead facts to support the conclusion that
 14 their reliance on the defendant's actions that caused the ascertainable loss was justifiable. *Yocca v.*
 15 *Pittsburgh Steelers Sports, Inc.*, 854 A.2d 425, 438 (Pa. 2004); *Riviello*, 2020 WL 1129956, at *4
 16 (“It is the plaintiff’s burden to prove justifiable reliance in the complaint”). As discussed above,
 17 Plaintiffs cannot meet this burden.

18 **5. Virginia Consumer Protection Act**

19 Plaintiff Lackey’s statutory claim fails because Virginia’s statute covers only “fraudulent
 20 acts or practices,” Va. Code § 59.1-200, something Plaintiffs have not plausibly alleged, *see supra*
 21 at IV.E.1., much less pled with the requisite particularity. *Wynn’s Extended Care, Inc. v. Bradley*,
 22 619 F. App’x 216, 220 (4th Cir. 2015). Plaintiff Lackey likewise fails to plead “actual damages,”
 23 *Polk v. Crown Auto, Inc.*, 228 F.3d 541, 543 (4th Cir. 2000), particularly given the lack of factual
 24 allegations showing that Lackey experienced any actual fraud, unauthorized charges, or spent any
 25 money on mitigation in relation to the incident. *See* CAC ¶¶ 199-200 (alleging only that Lackey
 26 spent time monitoring for fraudulent activity and suffered non-economic damages); *see also* Va.
 27 Code § 59.1-204(A) (solely permitting “an action to recover actual damages”). Finally, Plaintiff
 28 Lackey cannot bring this claim on behalf of a class. *See Casey v. Merck & Co., Inc.*, 722 S.E.2d

842, 846 (Va. 2012).

6. Plaintiffs' Minnesota Statutory Claims Are Inadequately Pled

To state a claim under the Minnesota Deceptive Trade Practices Act ("Minnesota DTPA") and Minnesota Consumer Fraud Act ("Minnesota CFA"), the Minnesota Plaintiffs must allege that Caesars engaged in deceptive or misleading practices in connection with the sale or advertisement of "merchandise." *E-Shops Corp. v. U.S. Bank Nat. Ass'n*, 678 F.3d 659, 665 (8th Cir. 2012) (recognizing that both the Minnesota DTPA and the Minnesota CFA require that the plaintiff plead false, deceptive or misleading conduct by the defendant in connection with the sale of merchandise). Plaintiffs' claims are defective because they hinge entirely on allegations of fraud relating to "security and privacy measures," *see e.g.*, CAC ¶ 507, but Caesars is not in the business of selling data security services. *See Mekhail*, 2024 WL 1332260, at *6 (plaintiff "alleges a misrepresentation related to data privacy, but [the defendant] is not in the business of providing data privacy services"); *Kuhns*, 868 F.3d at 719 (rejecting argument that representations relating to data security measures can form the basis for a claim under Missouri's parallel consumer fraud act where defendant offered "brokerage services," but "did not sell data security services"). Because neither claim is based on Caesars' actual services, they should be dismissed.

Plaintiffs' Minnesota DTPA claim fails for an additional reason—because the statute only permits injunctive relief, Plaintiffs must allege a likelihood of future deception or harm. *See Johnson v. Bobcat Co.*, 175 F. Supp. 3d 1130, 1140 (D. Minn. 2016) (recognizing that the sole statutory remedy for a Minnesota DTPA claim is injunctive relief). Here, the only future harm Plaintiffs articulate is from the Attack itself that has already occurred, and not from any future activity on the part of Caesars. *See Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 773 (C.D. Ill. 2020) (dismissing Minnesota DTPA claim because, "[w]hile Plaintiffs argue that Defendant's misrepresentations leave them open to a future risk of additional fraudulent activity, this is not the type of harm that the Court is able to issue an injunction against."); *In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *27 (D.N.J. Dec. 16, 2021) (dismissing claim under the Minnesota DTPA for failure to allege likelihood of future harm or deception by the defendant). Plaintiffs do not allege any facts suggesting they are likely to be

deceived again by Caesars’ ongoing conduct—their allegations concern Caesars’ past conduct. Plaintiffs also acknowledge that Caesars paid a ransom to secure the deletion of affected customers’ data, and cite to Caesars’ Form 8-K that makes clear that Caesars has already implemented enhanced security measures. Therefore, injunctive relief is not warranted and the claim should be dismissed.

7. Plaintiffs’ Illinois Statutory Claims Fail

Plaintiffs’ claims under the Illinois Deceptive Trade Practices Act (“Illinois DTPA”) and Illinois Consumer Fraud Act (“Illinois CFA”) fail for numerous reasons. *First*, like its Minnesota counterpart, the Illinois DTPA only permits injunctive relief and requires a plaintiff to allege a likelihood of future deception or harm. *See Kljajich v. Whirlpool Corp.*, 2015 WL 12838163, at *5 (N.D. Ill. Sept. 25, 2015) (the “only remedy under the [Illinois DTPA] is injunctive relief”); *Popp v. Cash Station, Inc.*, 244 Ill. App. 3d 87, 98 (1st Dist. 1992) (the Illinois DTPA was “enacted to prohibit unfair competition and was not intended to be a consumer protection statute”) (citation omitted); *Demedici v. CVS Health Corp.*, 2017 WL 569157, at *2 (N.D. Ill. Feb. 13, 2017) (dismissing Illinois DTPA claim and noting that “the problem inherent in . . . consumer actions” is that “[o]rdinarily, the harm has already occurred, thus precluding a suit for injunctive relief”) (citation omitted). As detailed above, Plaintiffs’ allegations relate strictly to prior conduct by Caesars, and not a risk of future fraud or deception.

Second, Plaintiffs’ Illinois CFA claim is defective because Plaintiffs do not allege any ascertainable damages. The Illinois CFA “requires ‘actual damages’ before a private litigant can bring suit.” *Lewert v. P.F. Chang’s China Bistro, Inc.*, 819 F.3d 963, 969 (7th Cir. 2016); *see also Moyer v. Michaels Stores, Inc.*, 2014 WL 3511500, at *7 (N.D. Ill. July 14, 2014). None of the seven Illinois Plaintiffs allege actual, ascertainable damages. Six of them allege nothing more than lost time, such as time spent “monitoring . . . credit card and checking account statements” and dealing with “disruptive [spam] phone calls.” *See, e.g., CAC* ¶¶ 49, 59, 69, 80, 90, 109. Only Plaintiff Stacy alleges something more—claiming that an unauthorized actor “attempt[ed] to purchase a car and a Verizon phone” with a credit card opened in her name (*Id.* ¶ 102)—but she does not allege that the “attempt” was successful or that it caused her economic loss.

1 *Third*, a plaintiff suing under the Illinois CFA “cannot maintain an action . . . when the
2 plaintiff does not receive, directly or indirectly, communication or advertising from the defendant.”
3 *De Bouse v. Bayer*, 235 Ill. 2d 544, 555 (2009). None of the Illinois Plaintiffs allege that they saw,
4 let alone were deceived by, any specific statement or advertisement from Caesars relating to its
5 data security practices.

6 **8. Plaintiffs’ Claim Under New York General Business Law § 349 Fails**

7 As detailed above, Plaintiffs fail to allege a materially misleading act to support their claim
8 under New York GBL § 349. To adequately plead a GBL § 349 claim, the complaint must make
9 “reference to the specific acts, representations and/or omissions that [the plaintiff] claims are
10 deceptive,” and further allege “why these acts were deceptive.” *Horowitz v. Stryker Corp.*, 613 F.
11 Supp. 2d 271, 287 (E.D.N.Y. 2009). The New York Plaintiffs identify no representation or
12 omission by Caesars that was deceptive or misleading in any way. Even generalized statements
13 about data security—which Plaintiffs do not even allege here—are not actionable material
14 misrepresentations when they would not mislead a reasonable person. *See Yuille*, 686 F.Supp.3d
15 at 346 (A “reasonable consumer could understand the statements alleged in the Complaint to
16 suggest that Uphold deployed specific security protocols that it believed to be reasonably adequate,
17 but the statements cannot be read to provide an assurance that there would be no circumstances
18 under which Uphold’s security systems would fail or that its accounts would be invulnerable to
19 third-party attacks.”); *Abdale v. N. Shore Long Island Jewish Health Sys., Inc.*, 49 Misc. 3d 1027,
20 1039 (Sup. Ct. Queens Cnty. 2015) (dismissing GBL § 349 claim based on health system privacy
21 policy). When, as here, “the allegations” in the complaint “are insufficiently specific to establish
22 a deceptive practice,” “[c]ourts routinely dismiss claims under GBL § 349.” *Woods v. Maytag Co.*,
23 2010 WL 4314313, at *16 (E.D.N.Y. Nov. 2, 2010); *see also Troy v. Am. Bar Ass’n*, 2024 WL
24 1886753, at *5-6 (E.D.N.Y. Apr. 30, 2024) (dismissing GBL § 349 claim in data breach case).

25 The New York Plaintiffs also posit that Caesars’ alleged failures to “comply with common
26 law and statutory duties” imposed by the FTC Act, “HIPAA,” (42 U.S.C. § 1320d) and “COPPA”
27 15 U.S.C. §§ 6501-6505 constitute a violation of GBL § 349. CAC ¶ 529. But none of these statutes
28 have a private right of action and thus “may not serve as [a] predicate[] for § 349 claims.” *See*

Rider v. Uphold HQ Inc., 657 F.Supp.3d 491, 500 (S.D.N.Y. 2023). Nor do the CAC’s nonsensical references to HIPAA or COPPA make any sense, as there are no allegations that Caesars is a “Covered Entity” or “Business Associate” under HIPAA or that the Attack involved any personal health information, nor is there any suggestion that Plaintiffs are under 13 years old or that personal information of children was impacted by the Attack (as would be necessary to implicate COPPA).

V. CONCLUSION

Caesars accordingly requests that the Court dismiss the Consolidated Class Action Complaint, with prejudice.

Dated: September 12, 2024.

MCDONALD CARANO LLP

/s/Adam Hosmer-Henner

Adam Hosmer-Henner (NSBN 12779)

Chelsea Latino (NSBN 14227)

Jane Susskind (NSBN 15099)

100 West Liberty Street, Tenth Floor

Reno, Nevada 89501

Telephone: (775) 788-2000

ahosmerhenner@mcdonaldcarano.com

clatino@mcdonaldcarano.com

jsusskind@mcdonaldcarano.com

LATHAM & WATKINS LLP

Serrin Turner (admitted *pro hac vice*)

1271 Avenue of the Americas

New York, New York 10022

Telephone: (212) 906-1200

serrin.turner@lw.com

Attorneys for Defendant

Caesars Entertainment, Inc.